MODALITĂȚI DE IDENTIFICARE A VULNERABILITĂȚILOR ÎN PROCESUL DE MANAGEMENT AL INCIDENTELOR DE SECURITATE A INFORMAȚIILOR

Conf. univ. dr. Claudia CÂRSTEA
Academia Forțelor Aeriene „Henri Coandă”, Brașov
DOI: 10.55535/GMR.2023.1.7

Aplicarea instrumentelor și metodelor de îmbunătățire a eficacității sistemului de management al securității informației, prin detectarea și neutralizarea atacurilor cibernetice, blocarea atacurilor malware, ransomware, spammers și spam servers, devine o cerință sine qua non în gestiunea incidentelor de securitate a informației cu scopul minimizării impactului acestora asupra sistemelor informatice. Lucrarea furnizează informații privind impactul integrării cerințelor de securitate atât de necesare utilizatorilor de tehnologie informațională din sistemele militare. Culegerea informațiilor s-a realizat pe un eșantion statistic de 128 de studenți din academii militare din România, Bulgaria și Polonia. Metodele de cercetare sunt completate cu metode transversale (chestionarul, ancheta, observația) și observaționale.

Cuvinte-cheie: securitatea informației, confidențialitate, integritate, vulnerabilitate, sisteme informatice.

DESPRE MANAGEMENTUL SECURITĂȚII INFORMAȚIEI

Atunci când se vorbește despre securitatea informației, utilizatorul se gândește direct la aspectul confidențialității, ignorând integritatea și disponibilitatea informației. În astfel de situații, este important ca, în cadrul unei organizații, să se implementeze o serie de bune practici, prin care toate categoriile de utilizatori să fie familiarizate cu cele trei dimensiuni ale securității informațiilor: autenticitatea, non-repudierea și fiabilitatea.

Conform *Metodologiei și instrucțiunilor de completare a formularelor de raportare a incidentelor majore/Regulament 2/2020 privind măsurile de securitate referitoare la riscurile operaționale și de securitate*, *confidențialitatea* este proprietatea informației de a nu fi disponibilă persoanelor, entităților sau proceselor neautorizate, iar *integritate*a se referă la asigurarea acurateței și completitudinii metodelor prin care se realizează prelucrarea informațiilor.

Confidențialitatea este proprietatea informației de a nu fi disponibilă persoanelor, entităților sau proceselor neautorizate, iar integritatea se referă la asigurarea acurateței și completitudinii metodelor prin care se realizează prelucrarea informațiilor.

Cu toate acestea, de multe ori, există solicitări privind accesibilitatea la cererea unei entități autorizate a informațiilor care trebuie prelucrate și atunci, cu siguranță, va trebui să se stabilească în timp real atât oportunitatea solicitărilor, cât și disponibilitatea informațiilor raportat la cerințele specifice ale utilizatorilor.

Există instrumente care să asiste utilizatorii în luarea deciziei? Se consideră că da! Dar cum este selectat cel care se adaptează specificului activității desfășurate? Apreciem că, în procesul evaluării, ar trebui să fie luate în calcul următoarele criterii:

- autenticitatea – ca proprietate a unei entități de a fi ceea ce pretinde că este;
- non-repudierea – ca o capacitate de a demonstra apariția unui eveniment sau acțiune revendicate sau a entităților sale care le-au generat;
- fiabilitatea – ca proprietate a comportamentului și rezultatelor consecvente.

POLITICILE DE MANAGEMENT DE SECURITATE A UNEI ORGANIZAȚII ȘI AMENINȚĂRI ALE SISTEMELOR INFORMATICE

Sistemele informatice trebuie analizate și percepute împreună cu toate componentele acestora, pornind de la echipamentele hardware, baza informațională, baza software cu platforme și programe de aplicație, resursele umane cu toate categoriile de utilizatori și, nu în ultimul rând, modelele matematice pentru optimizare și creșterea eficienței și eficacității unui sistem informatic. De aici și până la un sistem de management eficient este un singur pas, pentru că există tot setul de elemente ale unei organizații care interacționează pentru stabilirea politicilor, îndeplinirea obiectivelor și desfășurarea proceselor necesare realizării acestora, îndeplinirea indicatorilor de performanță și a criteriilor de succes. Aceasta înseamnă că orice cauză potențială a unui incident nedorit poate determina afectarea unui subsistem, a unui sistem sau chiar a întregii organizații, moment în care vorbim despre amenințare. Acest lucru înseamnă că există potențial ca o anumită vulnerabilitate a sistemului să fie utilizată fie accidental, fie în mod intenționat.

Sistemele informatice trebuie analizate și percepute împreună cu toate componentele acestora, pornind de la echipamentele hardware, baza informațională, baza software cu platforme și programe de aplicație, resursele umane cu toate categoriile de utilizatori și, nu în ultimul rând, modelele matematice pentru optimizare și creșterea eficienței și eficacității unui sistem informatic.

Vulnerabilitatea se referă la slăbiciunea unui bun sau a unui instrument de control, care poate fi exploatată direct sau indirect de către una sau mai multe amenințări. De exemplu, orice defect sau slăbiciune în proiectarea, implementarea, operarea sau administrarea unui sistem poate fi exploatat pentru a viola politica de securitate a sistemului. Foarte importantă, în acest moment, devine estimarea corectă a riscului, adică a efectului unei incertitudini în atingerea obiectivelor. Elementele care trebuie să se regăsească în politicile de securitate coerente sunt următoarele:

- seturile de activități intercorelate, care transformă intrările în ieșiri, denumite frecvent *procese*;
- determinarea stării unui proces sau activitate – ceea ce înseamnă monitorizare.

Eșantionul selectat pentru studiul impactului implementării cerințelor de securitate a informațiilor, în urma anchetei și observației efectuate, se concretizează în 128 de studenți din academii militare din Europa (România, Bulgaria și Polonia), astfel: Academia Forțelor Aeriene *„Henri Coandă”* din Brașov (56 de studenți), Universitatea

Națională Militară din Veliko Târnovo (42 de studenți) și Universitatea de Studii Militare din Varșovia (30 de studenți).

Metodele de culegere a informațiilor se bazează pe chestionare, observație directă și interviu. Fiind o metodă de cercetare cantitativă, chestionarul a fost foarte util în acest caz, prin varietatea și targetul întrebărilor adresate.

Domeniul întrebărilor include securitatea rețelelor de calculatoare, încrederea în tehnologie și managementul riscurilor, politica utilizării stick-urilor, configurarea platformelor, accesul utilizatorilor, lucrul de la distanță și importanța educării informaționale și cibernetice a utilizatorilor. Studenții care au răspuns întrebărilor aveau trei variante de răspuns la fiecare întrebare: *NU, DA, Este posibil*.

Scopul direct al acestei cercetări este înțelegerea barierelor și riscurilor, adoptarea unui comportament riguros și responsabil în utilizarea informațiilor pe mediile de stocare, înțelegerea strategiilor de diminuare a riscurilor, comportamentul în cazul apariției unui incident de securitate, precum și responsabilitățile privind planificarea resurselor pentru a răspunde unui incident. Scopul indirect al cercetării îl reprezintă conștientizarea utilizatorilor în ceea ce privește contextul general de întrebuințare a unui sistem informatic.

Agenția Națională pentru Securitatea Sistemelor Informatice, în *„Codul de bune practici pentru securitatea sistemelor informatice și de comunicații”* (2022, p. 4), promovează formarea și dezvoltarea unei culturi organizaționale care să înțeleagă necesitatea gestionării riscului ca element inevitabil în desfășurarea activității și în luarea deciziilor.

GÂNDIREA MILITARĂ ROMÂNEASCĂ

Scopul direct al acestei cercetări este înțelegerea barierelor și riscurilor, adoptarea unui comportament riguros și responsabil în utilizarea informațiilor pe mediile de stocare, înțelegerea strategiilor de diminuare a riscurilor, comportamentul în cazul apariției unui incident de securitate, precum și responsabilitățile privind planificarea resurselor pentru a răspunde unui incident. Scopul indirect al cercetării îl reprezintă conștientizarea utilizatorilor în ceea ce privește contextul general de întrebuințare a unui sistem informatic.

CONTEXTUL ACTUAL AL DEZVOLTĂRII EXPONENȚIALE A DIGITALIZĂRII DEVINE UN MAGNET AL ATACURILOR CIBERNETICE

Firmele de securitate informatică anticipează că atacurile vor deveni din ce în ce mai sofisticate, cu consecințe devastatoare pentru activitățile oamenilor și pentru companii, ca urmare cunoașterea trendului actual al manifestărilor amenințărilor informatice permite organizarea unor măsuri tehnice și organizatorice ce trebuie luate de către organizații pentru protejarea informațiilor. Ne referim aici la mai multe vulnerabilități cu impact mai mare asupra sistemelor informatice, precum și la numărul vulnerabilităților raportate care,

cu siguranță, va crește, conform monitorizărilor din ultimii ani. (*Infosfera*, nr. 2/2021, p. 49).

Un prim factor *„magnet”* îl reprezintă utilizarea din ce în ce mai largă a programelor de aplicație de tip *„open-source”*, fapt ce determină creșterea riscului de a deveni mai vulnerabili în fața atacatorilor. Tutorialele privind instrumentele de atac și apărare sunt disponibile acum tuturor utilizatorilor, ceea ce determină creșterea gradului de expunere la risc.

Tehnicile de inginerie socială, inteligența artificială și dezvoltarea competențelor în depistarea erorilor fizice sunt, de asemenea, factori care favorizează creșterea eficacității atacurilor informatice. În același timp, este de așteptat ca infractorii să își adapteze metodele de atac, căutând noi modalități prin care să amenințe sistemele și devenind din ce în ce mai greu de identificat.

Tehnicile de inginerie socială, inteligența artificială și dezvoltarea competențelor în depistarea erorilor fizice sunt, de asemenea, factori care favorizează creșterea eficacității atacurilor informatice. În același timp, este de așteptat ca infractorii să își adapteze metodele de atac, căutând noi modalități prin care să amenințe sistemele și devenind din ce în ce mai greu de identificat.

Sunt utilizate dispozitive din ce în ce mai inteligente și comportamentul utilizatorilor este din ce în ce mai nesigur și neprotejat. Andrea Radu, în articolul *„Securitate informatică”* (2019), estima un număr de 20 de miliarde de dispozitive inteligente conectate. Soluțiile de protecție, securitate și confidențialitate se vor îndrepta în mod evident către respectarea de standarde privind producerea dispozitivelor, respectarea restricțiilor de integritate privind colectarea și procesarea datelor și, nu în ultimul rând, asigurarea unui proces de mentenanță a sistemului informatic adaptat cerințelor informaționale ale tuturor utilizatorilor.

Accentul se va îndrepta spre respectarea drepturilor la intimitate, prin restricții impuse producătorilor de software și printr-o legislație coerentă.

Criptarea informațiilor și protejarea activității online a tuturor categoriilor de utilizatori sunt cerințe fundamentale în utilizarea aplicațiilor informatice. Dezvoltarea exponențială a tuturor domeniilor economice, a internetului obiectelor/Internet of things, a sistemelor de tip big data, a tehnologiilor de tip cloud și a digitalizării sistemelor este însoțită de o creștere a expunerii vulnerabilităților, permițând actorilor rău-intenționați să vizeze din ce în ce mai multe surse de exploatare cibernetică. În acest context, strategia de securitate a informației definită de fiecare organizație reprezintă planul care integrează obiectivele majore ale securității informatice, politicile și secvențele de acțiune ale organizației într-un sistem coeziv, unitar. Ea reprezintă

un document întocmit de către organizație și cuprinde o evaluare a amenințărilor informatice, precum și un set de contramăsuri pentru anihilarea acestora, care sunt asigurate financiar. Strategia este văzută, în acest context, ca un mijloc de a influența mediul intern al organizației prin selectarea atentă a mijloacelor de control intern.

REZULTATELE CERCETĂRII ȘI TENDINȚE ÎN IMPLEMENTAREA TEHNICILOR ȘI METODELOR DE SECURITATE A INFORMAȚIEI ÎN SISTEMELE MILITARE

Amenințările din interiorul organizațiilor pot duce la incidente de securitate, ceea ce înseamnă că un utilizator educat este un element cheie în cultura de securitate cibernetică a fiecărei organizații. Implementarea bunelor practici de securitate cibernetică este o cerință obligatorie în contextul actual al utilizării tehnologiei. Adoptarea unei strategii a securității informatice de către o organizație crește considerabil calitatea programului de securitate a informației, cu condiția existenței unei legături strânse între aceasta și strategia organizației. Strategia securității informației nu este definită în sine, ci este o orientare a politicilor de securitate, a controlului și auditului de securitate și a managementului sistemului de securitate. Obiectivele de securitate a informației trebuie să fie consistente în raport cu politica de securitate a informației, să fie măsurabile (dacă se poate), să ia în considerare cerințele aplicabile de securitate a informației și rezultatele evaluării și tratării riscului, să fie comunicate și să fie actualizate după cum este necesar.

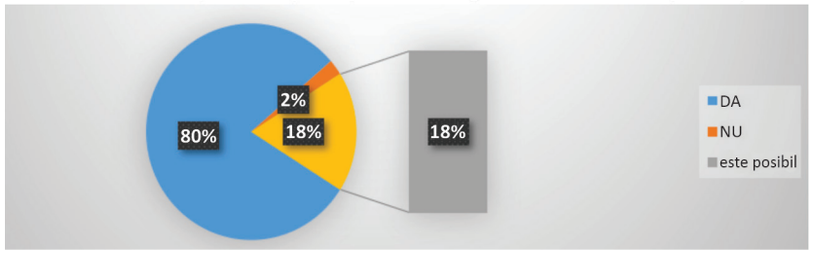
Implementarea bunelor practici de securitate cibernetică este o cerință obligatorie în contextul actual al utilizării tehnologiei. Adoptarea unei strategii a securității informatice de către o organizație crește considerabil calitatea programului de securitate a informației, cu condiția existenței unei legături strânse între aceasta și strategia organizației. Strategia securității informației nu este definită în sine, ci este o orientare a politicilor de securitate.

Cercetarea efectuată scoate în evidență punctele vulnerabile în implementarea bunelor practici de securitate cibernetică. În acest context, criteriile principale de evaluare a vulnerabilităților sistemelor informatice pot fi formulate și reprezentate grafic, astfel:

- *Securizarea stațiilor de lucru conectate la rețele este o condiție esențială pentru asigurarea confidențialității (Graficul 1).*
- *Criptarea datelor clasificate este importantă (Graficul 2).*
- *Gestionarea parolelor și utilizarea algoritmilor complecși pentru modificarea periodică a acestora (Graficul 3).*
- *Utilizarea de conturi cu drepturi limitate (Graficul 4).*
- *Sincronizarea datelor cu echipamente mobile (Graficul 5).*
- *Dezactivarea conexiunilor neutilizate pe echipamentele mobile (Graficul 6).*

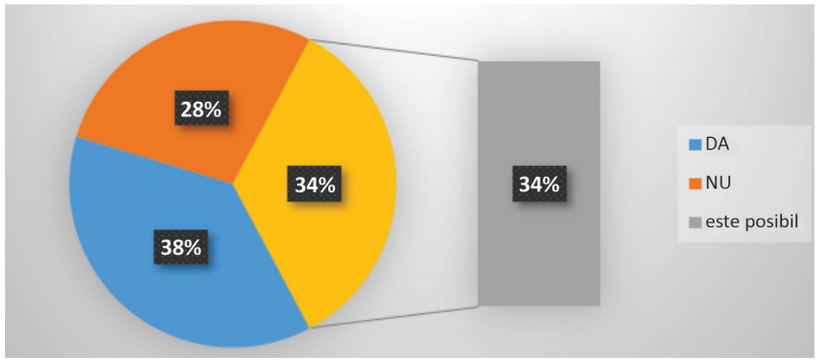
- *Distribuirea informațiilor personale (Graficul 7).*
- *Utilizarea unor medii de stocare verificate (Graficul 8).*
- *Conexiuni securizate de date (Graficul 9).*
- *Urmărirea accesului terților la date în rețele wireless (Graficul 10).*
- *Instalare de soluții antivirus actualizate (Graficul 11).*
- *Instalare de aplicații firewall (Graficul 12).*
- *Raportarea incidentelor de securitate (Graficul 13).*
- *Utilizarea unei liste albe a aplicațiilor (Graficul 14).*
- *Restricționarea conținutului web (Graficul 15).*
- *Realizarea evaluării de risc și de expunere la vulnerabilități (Graficul 16).*

Securizarea stațiilor de lucru conectate la rețele este o condiție esențială pentru asigurarea confidențialității



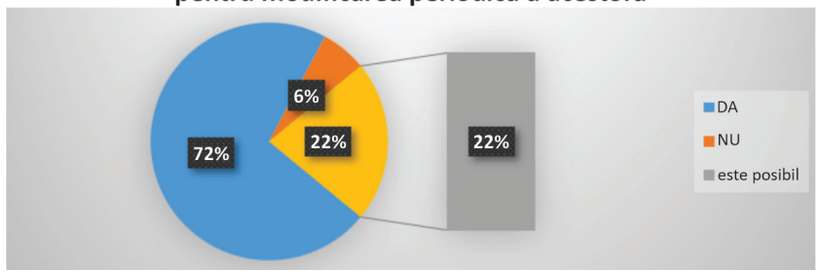
Graficul 1

Criptarea datelor clasificate este importantă



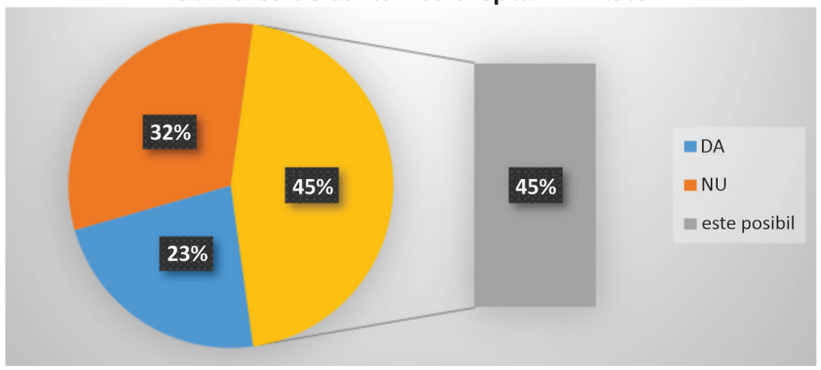
Graficul 2

Gestionarea parolelor și utilizarea algoritmilor complecși pentru modificarea periodică a acestora



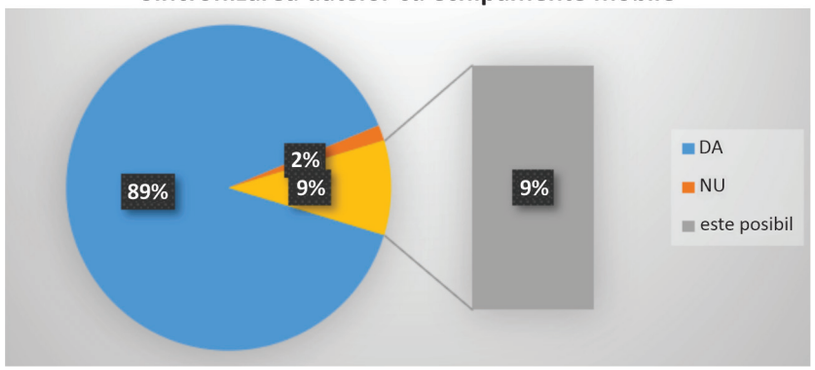
Graficul 3

Utilizarea de conturi cu drepturi limitate

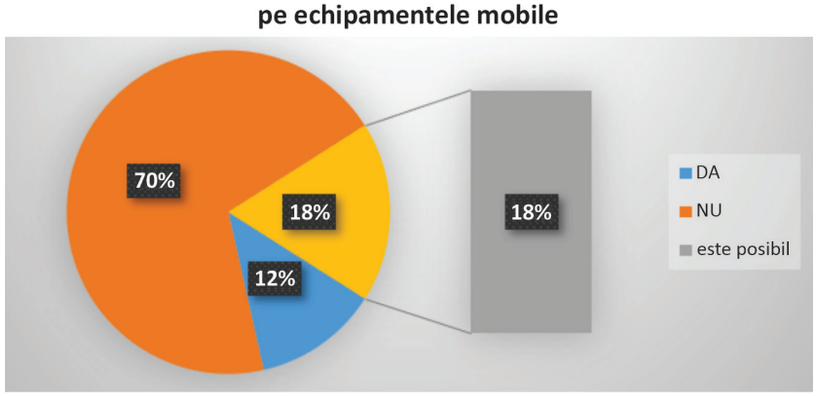


Graficul 4

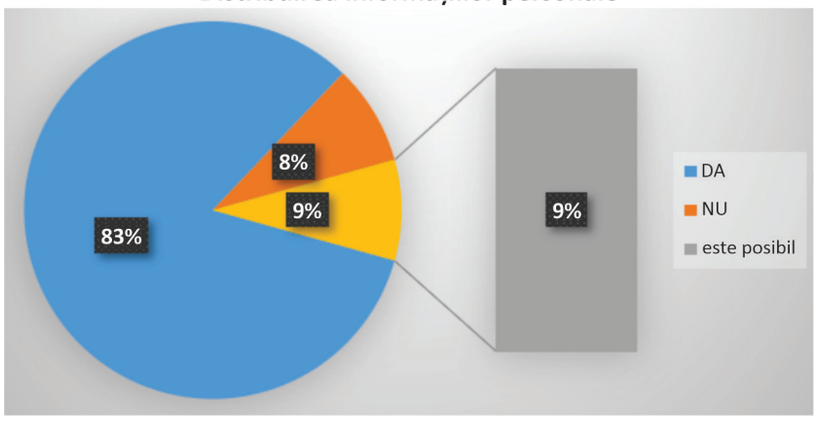
Sincronizarea datelor cu echipamente mobile



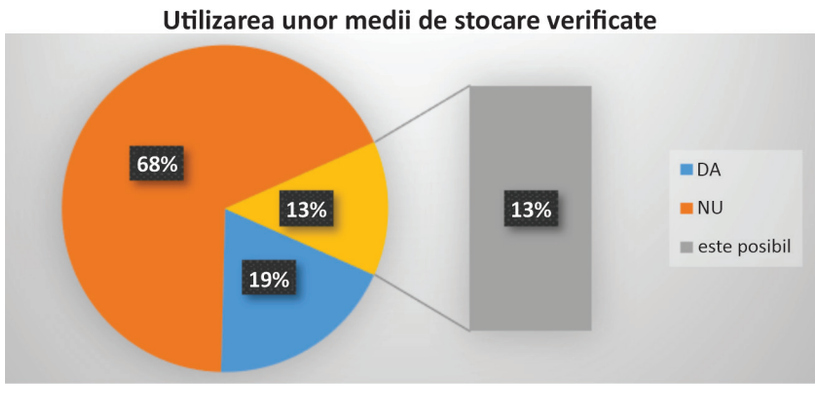
Graficul 5



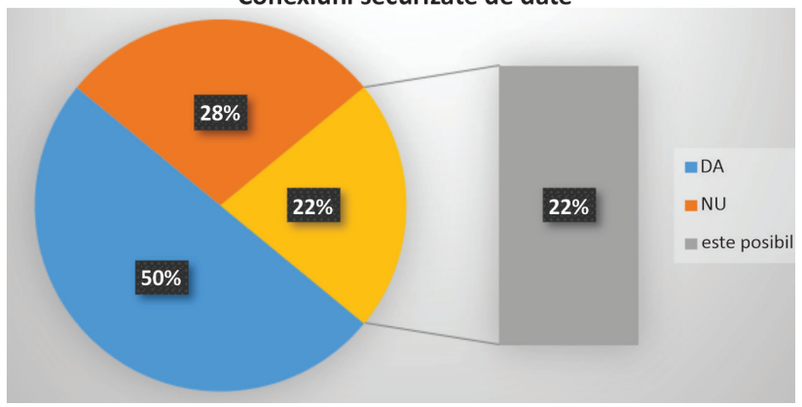
Graficul 6



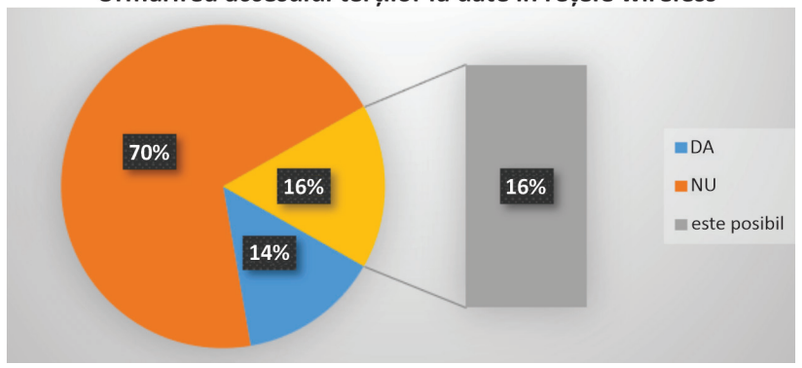
Graficul 7



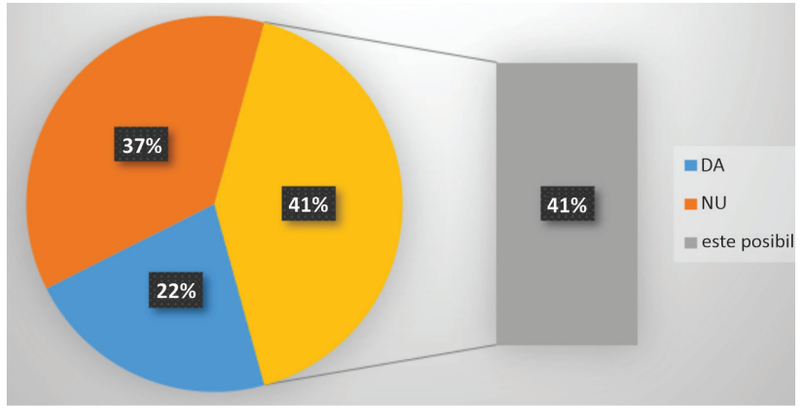
Graficul 8



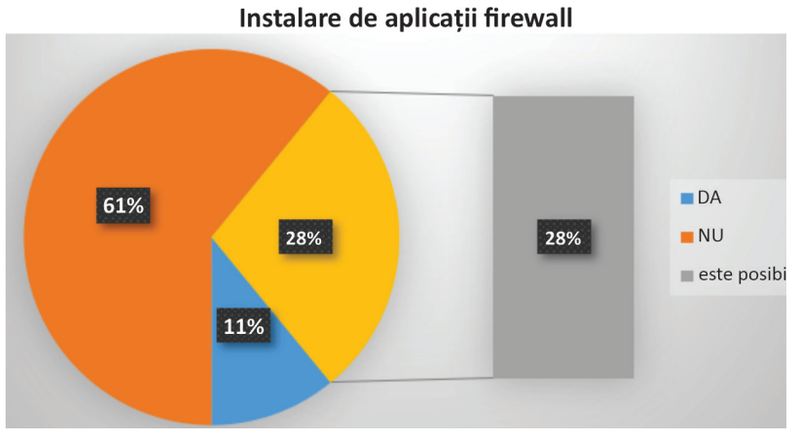
Graficul 9



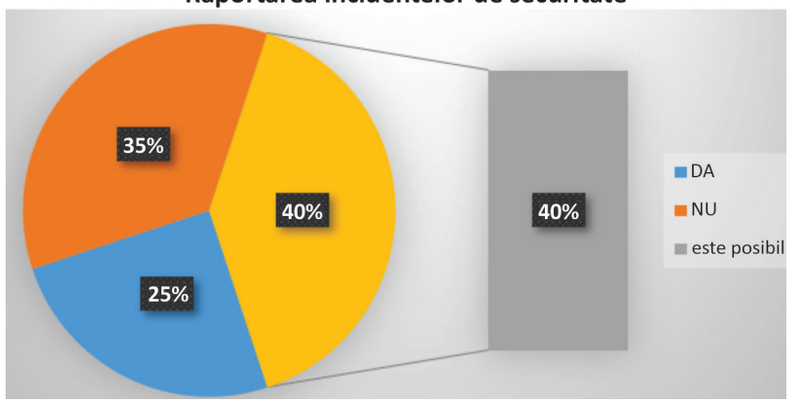
Graficul 10



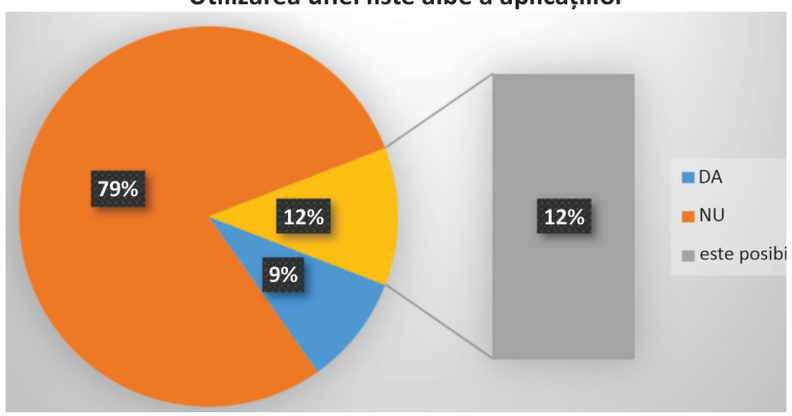
Graficul 11



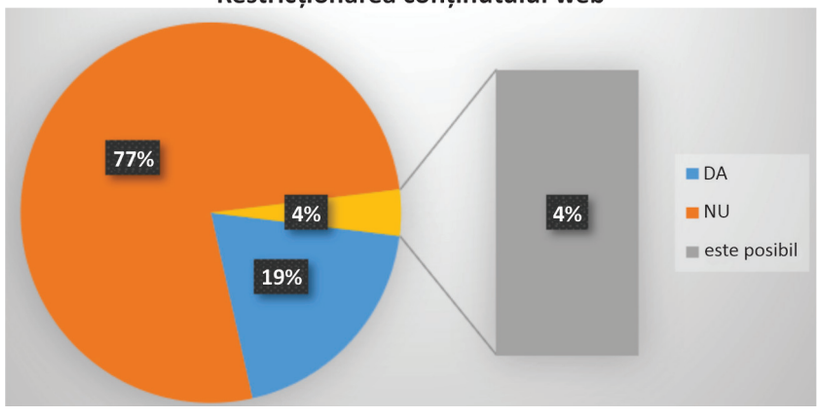
Graficul 12



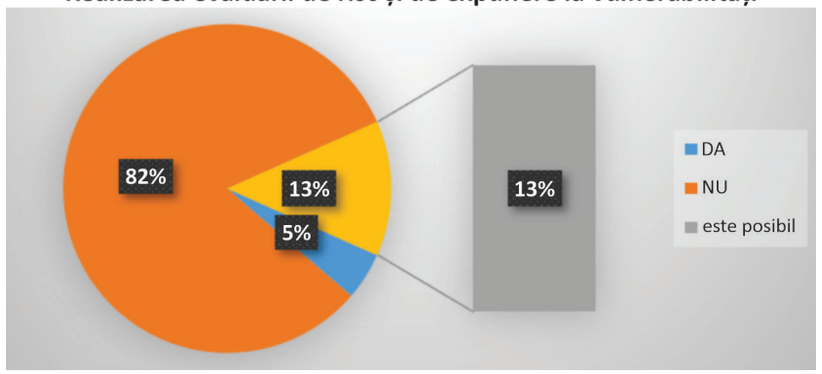
Graficul 13



Graficul 14



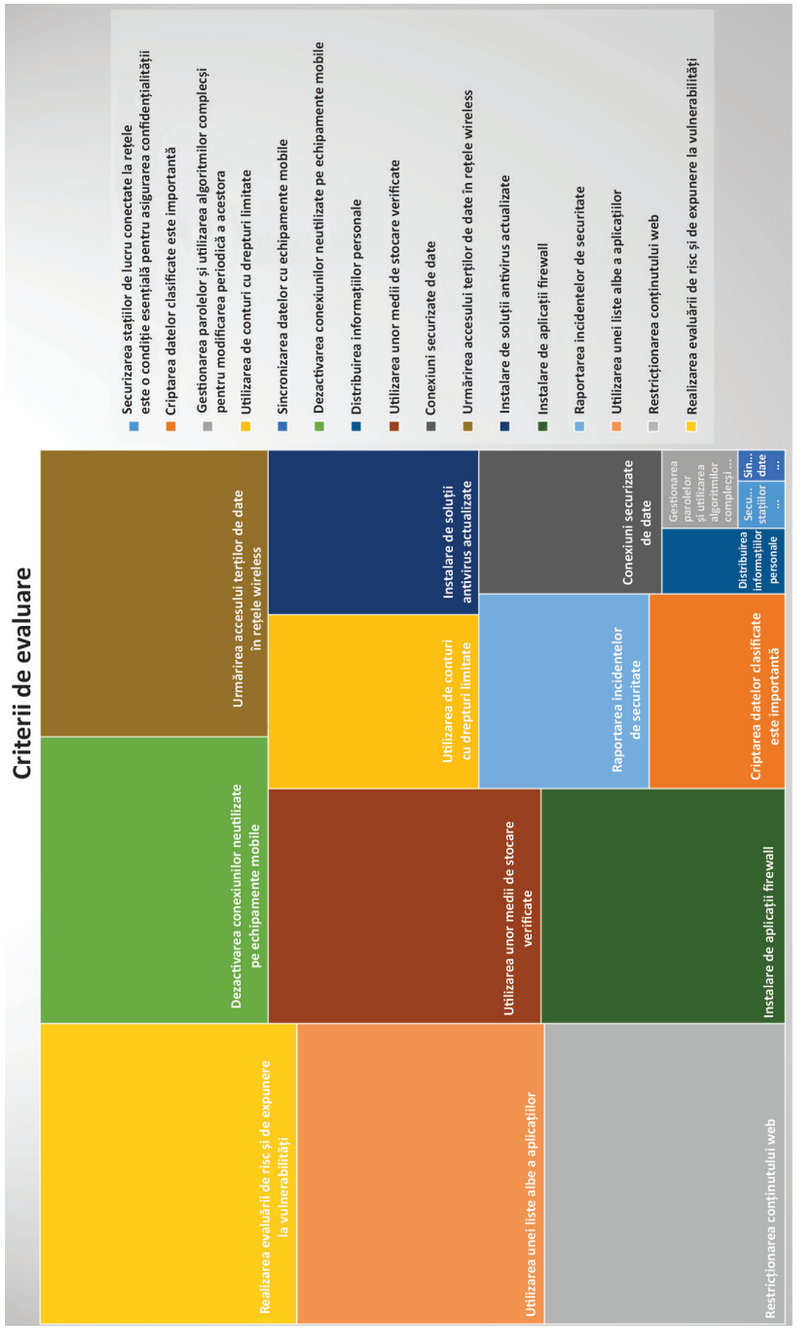
Graficul 15



Graficul 16

Rezultatul care sintetizează criteriile de evaluare a riscului de securitate a informațiilor *(Graficul 17)* reliefează în mod clar și coerent punctele vulnerabile în securitate. Preluarea acestor informații permite stabilirea unor strategii clare de identificare și minimizare a vulnerabilităților sistemelor informatice implementate. În mare măsură, lipsa disciplinei în utilizarea și sincronizarea dispozitivelor mobile și a rețelelor wireless mărește în proporție de 70% riscurile de securitate a informațiilor. Utilizatorii finali se expun, astfel, intenționat unor riscuri, prin nerespectarea regulilor și principiilor generale de securitate, fără să se gândească la repercusiunile acțiunilor lor imprudente.

Lipsa disciplinei în utilizarea și sincronizarea dispozitivelor mobile și a rețelelor wireless mărește în proporție de 70% riscurile de securitate a informațiilor. Utilizatorii finali se expun, astfel, intenționat unor riscuri, prin nerespectarea regulilor și priincipiilor generale de securitate, fără să se gândească la repercusiunile acțiunilor lor imprudente.



Grafic 17

ALERTĂ PRIVIND INCIDENTELE DE SECURITATE DE TIP LEBĂDA NEAGRĂ (BLACK SWAN)

Matematicianul Nassim Nicholas Taleb precizează că incidentele de tip *Lebăda neagră/„Black Swan”* sunt rare, ca evenimente; ele nu pot fi prevăzute, dar sunt evenimente neplăcute, cu impact major, și pot fi explicate numai după ce apar și produc efecte. De exemplu, pot fi considerate incidente de tip *„Black Swan”*: explozia rețelei internet, Primul Război Mondial, dizolvarea Uniunii Sovietice, evenimentul de la 11 septembrie 2001, dezastrul nuclear de la Fukushima Daiichi. (Mambet, 2012).

Pandemia COVID-19 a accelerat dezvoltarea mediului și a *„lumii”* virtuale, chiar acceptarea ei în diferite sisteme în care se presupunea că este imposibil de utilizat. Este, oare, COVID-19 un incident de tip *„Black Swan”*? Răspunsul este NU, pentru că se pare că a fost un dezechilibru între componenta operațională și cea de securitate medicală (*Infosfera,* p. 67). Ne întrebăm totuși dacă incidente de tip *„Black Swan”* vor mai apărea? Cu siguranță, da! Este doar o problemă de timp. Cu toate acestea, pandemia COVID-19 a accelerat dezvoltarea lumii virtuale și a creat un dezechilibru vizibil între utilizarea tehnologiei și componenta de securitate, care duc, în mod evident, la incidente de securitate predictive, de tip *„White Swan”*. Un model de securitate care poate fi utilizat cu succes este algoritmul de criptare, care este un model matematic implementat pentru securitatea informațiilor. Produsele criptografice se pot utiliza pentru a proteja datele în sistemele de comunicație sau în aplicații specifice. Algoritmul de evaluare este ușor de înțeles de către utilizatori și facil de implementat, raportat la resursele hardware și software de care unitatea dispune.

Evaluarea modulelor criptografice se poate realiza folosind standardul FIPS 140-2 echiv ISO19790; 4 niveluri de securitate; cerințe de securitate funcționale și cerințe specifice de securitate, cum ar fi: specificații pentru modulul criptografic, porturi și interfețe dedicate modulului criptografic, roluri, funcții și autentificări specifice, securitate fizică, mediu operațional coerent, administrarea coerentă a cheilor de criptare, autotestări, asigurarea proiectului, diminuarea altor atacuri – ceea ce înseamnă un management al riscurilor eficient.

Pandemia COVID-19 a accelerat dezvoltarea lumii virtuale și a creat un dezechilibru vizibil între utilizarea tehnologiei și componenta de securitate, care duc, în mod evident, la incidente de securitate predictive, de tip „White Swan”. Un model de securitate care poate fi utilizat cu succes este algoritmul de criptare, care este un model matematic implementat pentru securitatea informațiilor.

Criterii comune se regăsesc în standardele echivalente ISO15408, astfel:

- Trusted Computer System Evaluation Criteria, 1983, NSA;
- Canadian Trusted Computer Product Evaluation Criteria, 1993, Communications Security Establishment pentru a furniza criterii de evaluare comune ale produselor IT;
- Information Technology Security Evaluation Criteria (mai 1990), în Franța, Germania, Olanda și Marea Britanie;
- Common Criteria, 31 de membri.

Rămâne totuși întrebarea dacă le vom înlocui cu *„Cyber security Act”*?

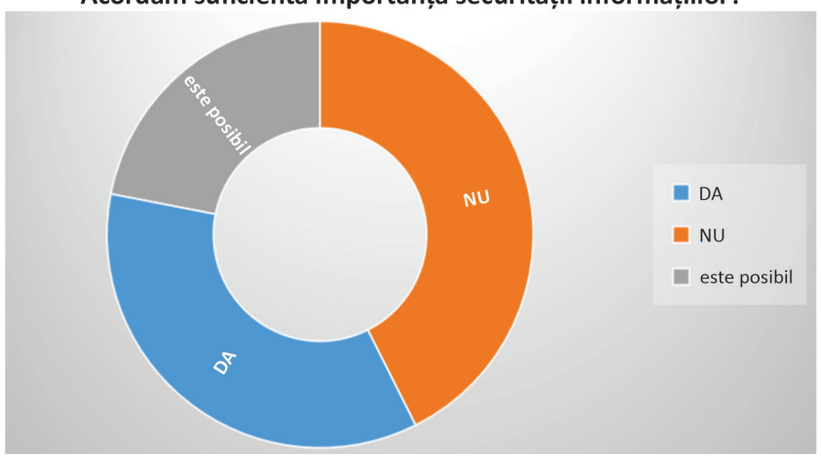
Cerințele de asigurare a securității informațiilor trebuie să fie formulate în mod clar, corect și coerent de către fiecare organizație în parte, explicate periodic utilizatorilor finali, prin accentuarea următoarele aspecte: dezvoltarea aplicațiilor; cunoașterea ciclului de viață a unui sistem informatic; actualizarea cunoștințelor privind instrumente utilizate în securitatea informației; evaluarea și analiza vulnerabilităților.

CONCULZII

Rezultatele acestor cercetări statistice reflectă punctele vulnerabile și modul în care utilizatorii abordează conceptele de securitate, concretizate în acțiuni. Astel, putem conchide că cerințele de asigurare a securității informațiilor trebuie să fie formulate în mod clar, corect și coerent de către fiecare organizație în parte, explicate periodic utilizatorilor finali, prin accentuarea următoarele aspecte:

- Dezvoltarea aplicațiilor – design arhitectural, specificații funcționale, proiectare, reprezentare implementare, modelare politici de securitate.
- Îndrumare privind regulile de utilizare sigură a aplicațiilor.
- Cunoașterea ciclului de viață a unui sistem informatic: definirea ciclului de viață, domeniul de aplicare a managementului configurației și capabilități, securitate în timpul dezvoltării, securitatea livrării, flux de remediere, instrumente și tehnici.
- Actualizarea cunoștințelor privind instrumente utilizate în securitatea informației: testare funcțională (planuri, proceduri și înregistrări), analiza acoperirii testelor, analiza adâncimii testului, testare independentă.
- Evaluarea și analiza vulnerabilităților.

Cuvintele sunt insuficiente atunci când analizăm *graficul 18*, generat pe baza rezultatelor centralizatoare din chestionarul aplicat pe grupul țintă. Imaginea este relevantă și, totodată, îngrijorătoare. Este evident că educația privind securitatea cibernetică este strict



Graficul 18

necesară și trebuie instrumentată. Utilizatorii finali nu acordă suficientă atenție securității informațiilor, de multe ori mergând pe principiul *„mie nu poate să mi se întâmple”* sau *„organizația în care lucrez mă protejează”*. Cercetarea va fi dezvoltată analizând și alte criterii, aplicând chestionarul pe categorii de utilizatori și categorii de vârstă specifice, țintind măsurile pentru minimizarea vulnerabilităților sistemelor informatice militare. Fragmentarea grupului țintă va permite, totodată, identificarea mai precisă a riscurilor în securitatea informațiilor.

REFERINȚE BIBLIOGRAFICE:

1. Mambet, C. (2012). *Abordarea transdisciplinară a gestiunii și managementului riscurilor și al proceselor decizionale*. Teză de doctorat, https://ciret-transdisciplinarity.org/biblio/biblio_pdf, accesat la 22 octombrie 2022.
2. Radu, A. (2019) *„Securitate informatică”*. În revista online asig.ro, https://www.1asig.ro/Securitate-informatica-Atacurile-vor-deveni-din-ce-in-ce-mai-sofisticate-in-2020-articol-3,102-62487.htm, accesat la 17 octombrie 2022.
3. *„Codul de bune practici pentru securitatea sistemelor informatice și de comunicații”* (2022). București.
4. European Union Agency for Cyber security (ENISA). Publications from the Threat Landscape 2020 Series, https://www.enisa.europa.eu/publications, accesat la 22 octombrie 2022.

5. European Union Agency for Law Enforcement Cooperation (EUROPOL). Publications and documents on cybercrime, https://www.europol.europa.eu/publications-documents, accesat la 12 octombrie 2022.
6. European Union Agency for Law Enforcement Training (CEPOL). E-Journals on cybercrime, https://www.cepol.europa.eu/science-research/journals/e-journals, accesat la 22 octombrie 2022.
7. *Infosfera* (2021). Revistă de studii de securitate și informații pentru apărare, anul XIII, nr. 2.
8. International Journal of Information Security and Cybercrime (IJISC), https://www.ijisc.com/, accesat la 22 octombrie 2022.
9. *Metodologia şi instrucţiunile de completare a formularelor de raportare a incidentelor majore/Regulament 2/2020 privind măsurile de securitate referitoare la riscurile operaționale și de securitate* (2020). În *Monitorul Oficial*, Partea I, nr. 115 din 14 februarie 2020, https://lege5.ro/Gratuit/gm3dcmzxhayq/regulamentul-nr-2-2020-privind-masurile-de-securitate-referitoare-la-riscurile-operationale-si-de-securitate-si-cerintele-de-raportare-aferente-serviciilor-de-plata?pid=310681889#p-310681889, accesat la 22 octombrie 2022.
10. National Association for Information Systems Security (ANSSI). Guide for securing computers and networks, https://cert.ro/vezi/document/ghid-bune-practici-pentru-securizarea-calculatoarelor-personale, accesat la 22 octombrie 2022.
11. National Cyberint Center within the Romanian Intelligence Service. Best practices guide for cybersecurity, https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf, accesat la 22 octombrie 2022.
12. Romanian Association for Information Security Assurance (RAISA). Considerations on challenges and future directions in cybersecurity, https://www.raisa.org/documents/CybersecurityRO2019.pdf., accesat la 12 octombrie 2022.
13. Romanian National Computer Security Incident Response Team (CERT-RO). Cybersecurity guides, https://cert.ro/doc/ghid, accesat la 7 octombrie 2022.
14. Checkmarx, https://www.checkmarx.com/, accesat la 22 octombrie 2022.
15. FIPS 140-2, https://csrc.nist.gov/publications/detail/fips/140/3/final, acceat la 22 octombrie 2022.
16. HCL (IBM) Appscan, https://www.hcltechsw.com/products/appscan, accesat la 7 octombrie 2022.
17. ISO 15408, https://www.iso.org/standard/50341.html, accesat la 7 octombrie 2022.

18. ISO 19790, https://www.iso.org/standard/52906.html, accesat la 7 octombrie 2022.
19. MBSA, Microsoft Baseline Security Analyzer, https://www.microsoft.com/en-us/security/blog/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer/, accesat la 7 octombrie 2022.
20. NIAP, https://www.niap-ccevs.org/, accesat la 7 octombrie 2022.
21. Vulnerability scanners NESSUS, https://www.tenable.com/products/nessus, accesat la 7 octombrie 2022.
22. https://www.commoncriteriaportal.org/, accesat la 12 octombrie 2022.