ABORDAREA SECURITĂȚII INFORMAȚIEI ÎN BAZA STANDARDELOR

STANDARDS-BASED INFORMATION SECURITY APPROACH

CZU: 004.056.5:006.35(100)ISO **https://doi.org/10.59295/spd2024n.97**

Tudor BRAGARU,
ORCID: 0000-0001-6356-2906
e-mail: theosnume@gmail.com
Universitatea de Stat din Moldova

Summary. *Many people mistakenly believe that information security (SI) and cyber security (SC) are completely different and that SC only boils down to technical-technological issues, settings, firewall rules, etc. In reality SI and SC are very close, and statistics show that the human problem predominates with a weight of about 70 to 95%. The purpose of this paper is to disprove some illusions/myths regarding SI/SC and elucidate their correct approach, with the reorientation from the paradigm based on software-technical-technological problems – towards organizational and management problems, based on generally accepted standards of good practices, without diminishing the importance of IT security and not limited to it. The work is carried out on the basis of an in-depth study of the modern trends in the organization and management of SI/SC with the analysis and synthesis of some recommendations based on bibliographic sources and the standards of best practices for the organization and management of SI/SC. The benefits of the SI/SC approach through the prism of good practice standards are multiple, generally recognized and confirmed by numerous results obtained in research, publications and the increase of the number of certifications of SI/SC management systems.*

Keywords: *Information security threats, ISO/IEC 27k family of standards, Security risks, Information security, Information security management system (SMSI).*

INTRODUCERE

Argument. În *societatea* informațională modernă bazată pe cunoaștere și pe e-transformarea bulversantă a afacerilor digitale, a e-industriei, a e-guvernării, a e-educației, a e-comunicațiilor etc., *securitatea informației/securitatea cibernetică a devenit vitală* pentru oameni, afaceri și orice alte entități, indiferent de țară, industrie, dimensiuni. Amenințările devin din ce în ce mai sofisticate, iar urmările realizării lor devin din ce în ce mai grave. Ca urmare, pentru a proceda corect în diferite situații, este important ca toată lumea să înțeleagă *importanța, tendințele, provocările și problemele majore ale securității informației/securității cibernetice, miturile/concepțiile greșite comune în domeniul SI/SC și realitățile*.

În prezenta lucrare termenii „*securitatea cibernetică”* și *„securitatea informației”* sunt utilizați cu sens interschimbabil potrivit contextului. Aceasta deoarece conceptul de „*securitate a informației”* se referă la orice informații, inclusiv digitale și pe suport de hârtie, este ceva mai larg decât SC, *ce constituie cca 95% din SI* și care se referă doar la informațiile digitale din spațiul cibernetic. Totodată, ambele concepte până în 2023 erau definite ca *„conservarea celor trei proprietăți primare/fundamentale ale informației: Confidențialitate, Integritate și Accesibilitate” (clauza 3.8. ISO/IEC 27000:2020 și clauza 4.20 ISO/IEC 27032:2012)* și câtorva proprietăți secundare bazate pe cele fundamentale, precum *autenticitatea, responsabilitatea, non-repudierea* și *fiabilitatea* . Diferența majoră dintre securitatea informației și securitatea cibernetică este elucidată în ultima ediție a standardului *ISO/IEC 27032:2023,* care definește SC ca *„protejarea oamenilor, a societății și a națiunilor de riscurile cibernetice”* în spațiul cibernetic *(concept conform clauzei 3.6 ISO/IEC 27100:2020).* Acest lucru este foarte important în contextul creșterii dependenței tot mai mari de tehnologie și de Internet, când SC devine de-a dreptul crucială. SC stabilește explicit relațiile între *securitatea Internet, securitatea web și securitatea rețelelor*, practic înglobându-le pe toate cele implicate cu atribuții de protecție a infrastructurilor informaționale *(dispozitive, aplicații, sisteme și date)* împotriva amenințărilor cibernetice asupra informației.

Actualitatea și importanța temei abordate este confirmată și de numeroase cercetări, de prezența acestei tematici pe agenda majorității absolute a conferințelor și forurilor științifice de nivel național și internațional, de numeroase statistici, unele dintre care sunt prezentate mai jos.

MATERIALE ȘI METODE

Există zeci de mituri comune răspândite [1, 2, 3], care împiedică buna înțelegere a SI/SC și care pot constitui o adevărată problemă în multe cazuri:

1. Securitatea cibernetică este o problemă doar tehnică-tehnologică.

2. Securitatea cibernetică este doar grija departamentului de IT (DIT); este doar pentru experți; nu este responsabilitatea mea.

3. Parolele puternice, firewall-uri și antivirus sunt suficiente pentru o bună SC.

4. Infractorii cibernetici nu vizează întreprinderile mici și mijlocii.

5. Conformitatea cu standardele și regulamentele în vigoare oferă suficientă SC.

6. Cumpărarea mai multor instrumente consolidează protecția securității cibernetice.

7. Testele regulate de penetrare asigură o SC suficientă.

8. Criptarea este bagheta magică pentru SI/SC.

9. Datele cu care operăm sau la care avem acces nu sunt valoroase.

10. Securitatea cibernetică necesită o investiție financiară mare și multe altele variații similare.

În continuare și doar pentru exemplificare sunt elucidate doar câteva dintre aceste mituri comune, iar pentru mai multe mituri și mai multe detalii a se vedea sursele citate.

Securitatea informației/SC rezidă preponderent în securitatea IC&T, este doar grija DIT *[1, mit 4], [3, mit 9],* **SC este doar o povară financiară** *[1, mit 19]. Absolut fals*. Într-adevăr, securitatea IC&T este veriga principală, de care depind foarte multe, dar nu toate. DIT este responsabil de implementarea și revizuirea politicilor de securitate, de monitorizarea rețelei, de aplicarea măsurilor concrete pentru a diminua multe dintre amenințările cibernetice, dar nu se poate ocupa de toate și nu poate fi responsabil pentru toți. În societatea modernă bazată pe IC&T, unde practic toată lumea utilizează diverse dispozitive electronice și gadgeturi conectate la Internet, SC nu mai rezumă doar în probleme tehnice, tehnologice, setări etc., ci a devenit o problemă preponderent umană, ce ține de comportamentul uman, de motivația și de cultura care influențează deciziile și acțiunile lor, de educația și împuternicirile lor și a tuturor părților interesate. Iar IT și preocupările DIT constituie doar o parte a SC, cea mai mare parte se referă la alți oameni și alte procese și la modul în care toate acestea interacționează cu IT și DIT. Trebuie luate în considerare *politicile organizaționale, procedurile și guvernanța*, care promovează sau împiedică eforturile de securitate și modul de aliniere a acestora cu scopurile și obiectivele de securitate. Astfel, pe măsură ce IC&T devin tot mai diversificate și utilizate, atacurile devin mai puțin concentrate pe mijloacele programo-tehnice, fiind țintite spre *factorul uman, considerat a fi cel mai vulnerabil*.

La investițiile în IC&T se adaogă investițiile legate de educația și instruirea continuă a personalului de toate nivelurile. La responsabilitatea DIT se adaogă responsabilitatea tuturor utilizatorilor IC&T de a fi vigilenți, de a cunoaște și înțelege provocările, vulnerabilitățile, riscurile de SI/SC și a celor mai bune practici în activitățile operaționale de *colectare, stocare, procesare, nimicire a informației* în condiții de siguranță. În final, *responsabilitatea aparține top managementului*, *care adoptă politici, regulamente, alocă resursele necesare* pentru asigurarea nivelului necesar al SI/SC. Ca urmare, SI/SC nu este/nu poate fi doar grija DIT, nu rezidă doar în securitatea IT, investițiile nu se referă doar la IT. Entitățile sunt nevoite să investească în educația, informarea-conștientizarea personalului privind cele mai recente provocări, tendințe, amenințări și vulnerabilități pentru ca să-și poată adapta și realiza strategiile de SI/SC de-a lungul timpului.

Securitatea informației/SC este un proiect care se termină; faci o singură dată setările pentru securizarea sistemelor și rețelelor și uiți de asta. *Și acesta este un sentiment absolut fals de SC,* deoarece mediul IC&T și ciberspațiul global sunt în continuă și bulversantă dezvoltare și transformare continuă, zilnic apar noi atacuri, riscuri, viruși. SC este un proces dinamic și continuu, care trebuie actualizat, îmbunătățit, monitorizat în mod constant, pentru ca controalele și măsurile de securitate să fie eficiente. Astfel, SI/SC nu este un proiect de o singură dată, ci un *ciclu continuu de planificare, dezvoltare/implementare, evaluare/verificare și îmbunătățire (cunoscut ca ciclu de îmbunătățire continuă Plan-Do-Check-Act, adoptat de toate standardele de management).*

Nu trebuie să ne facem griji prea mari cu privire la SC pentru că nu avem nimic de ascuns și/sau datele noastre (sau datele la care avem acces) nu sunt valoroase și/sau pentru că nu vizităm site-uri inoportune etc. *Această concepție greșită este foarte*

răspândită. De exemplu, se consideră că dacă nu vizionăm situri inoportune, malițioase – nu avem probleme de SC. Adevărul este că siturile web legitime pot fi compromise și infectate cu cod rău intenționat. Adesea, atacatorii profită de defectele browser-elor și plugin-urilor siturilor web [4]: *Peste 4,1 milioane de site-uri web au programe malware; Peste 18 milioane de site-uri web sunt infectate cu malware în fiecare săptămână; 97% dintre breșele de securitate exploatează plugin-uri Word Press.*

La fel există diverse **mituri și legende privind familia de standarde ISO27k** [5]. De exemplu, mulți consideră eronat că *seria se referă doar la două-trei standarde de bază*. Aceasta este absolut fals. Într-adevăr seria a debutat în 2000 cu un singur standard ISO/IEC 27002, ulterior a fost lansat standardul sistemic ISO/IEC 27001 (în 2005) privind sistemului de management al securității informației. Astăzi familia ISO27k cuprinde cca 80 de standarde implementate din cele circa 90 planificate pentru a înlesni implementarea SMSI. Multe dintre standarde au ajuns la ediția 4-5, fiind esențial revizuite și îmbunătățite. Actualizări importante ale standardelor pereche ISO/IEC 27001- ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27032 și altele au avut loc în anii 2022-2023, care au apropiat și mai mult aceste standarde, înlesnind maparea controalelor de SI/SC, Securitatea rețelelor, Internet, Web etc., inclusiv cu NIST, Top 18 CIS Critical Security Controls *(Center for Internet Security)*, care au înlocuit Top 20 SANS Critical Security Controls *(SysAdmin Network Systems)* și altele.

O altă iluzie se referă la egalarea conformității cu securitatea [1, 3, 5]**.** Certificarea de conformitate cu ISO/IEC 27001 este vitală pentru entitate, imaginea sa, operațiunile pe care le desfășoară etc., dar aceasta acoperă doar elementele de bază ale securității. Conformitatea nu oferă careva garanții asupra nivelului de securitate al organizației certificate și nici nu este odată pentru totdeauna. Certificatul confirmă doar că entitatea are implementat un SMSI care este conform într-un moment dat cu cerințele ISO/IEC 27001 în aria unui perimetru și a unei declarații SoA *(Statement of Applicability)* definite și doar pe o perioadă relativ scurtă, de cca un an. Dar informațiile și sistemele, inclusiv SMSI, inclusiv amenințările și riscurile evoluează continuu. Ca urmare, echipa de SC va trebui să răspundă nevoilor schimbătoare de securitate cibernetică.

Pentru a fi mai convingători, iată alte câteva statistici de securitate cibernetică [4]:

- 51% dintre companiile cu o politică BYOD au suferit o încălcare a datelor mobile;
- 92% din programele malware sunt livrate prin e-mail;
- 81% dintre încălcările de date se datorează parolelor slabe, furate sau implicite;
- La fiecare 39 de secunde un atacator vizează infrastructura de securitate cibernetică a unei afaceri; zilnic sunt create cca 300.000 de programe malware (estimativ);
- 68% dintre directorii executivi consideră că riscurile de securitate cibernetică cresc.

O mulțime de info-grafice, care înlocuiesc mii de cuvinte, pot fi găsite la Statista [6]. De exemplu „*Criminalitatea cibernetică se așteaptă să crească vertiginos în ur-*

mătorii ani”, de la 0,86 în 2018 la 13,62 trilioane de dolari SUA în 2028, adică de cca 16 ori in 10 ani! Statistici alarmante privind securitatea cibernetică a se vedea [7]. De exemplu, întreprinderile mici sunt deosebit de vulnerabile – de la 43 la 58 % dintre toate atacurile cibernetice sunt direcționate către acestea; 95% dintre toate încălcările de date includ elementul uman, implicat fie prin eroare, utilizare greșită a privilegiilor, utilizarea acreditărilor furate sau inginerie socială. Conform [8], trei moduri principale de atac cibernetic sunt *acreditările furate, phishing și exploatarea vulnerabilităților.*

Însă **a dezminți miturile și a speria cu statistici este puțin.** Pentru asigurarea SI/SC este necesară adoptarea unui cadru rezonabil de dezvoltare-implementare-monitorizare, care să fie:

- **Scalabil** – să poată fi dezvoltat simultan cu dezvoltarea afacerii, IC&T, sistemelor informaționale etc. și continuu adaptat la apariția noilor amenințări și riscuri;
- **Repetabil** – susținut de metodologii și procese iterative pe domeniile definite ale procesării informațiilor, cu oferirea de rezultate consistente și comparabile în timp sau între entități;
- **Defensiv** – să permită îmbunătățirea continuă bazată pe analiza riscurilor specifică contextului, utilizarea principiilor și controalelor auditabile, proceselor și cadrelor documentate și acceptate pentru gestionarea și controlul riscului;
- **Măsurabil** – să permită măsurarea capacității SI, ce oferă o imagine clară a stării programului de securitate și a capacităților de performanță, a îmbunătățiri continue definite în mod obiectiv de schimbările din mediile de risc sau de afaceri;
- **Durabil** – să fie centrat pe afacere, cu proceduri definite care să sprijine creșterea eficienței proceselor de afaceri și reducerea costurilor de conformitate pe ciclul de viață al informațiilor și adaptării la schimbările în mediile IT/IS și de afaceri.

Un asemenea cadru general acceptat este **abordarea securității informației în baza standardelor** de bune practici, cu sublinierea creșterii semnificației părții de management față de partea tehnică-tehnologică. Deoarece, în primul rând factorul uman a devenit semnificativ, iar în al doilea rând, standardele internaționale din domeniul securității informației, IT, IS, Internet, Web etc., dezvoltate și îmbunătățite de-a lungul anilor au reușit să **absoarbă cele mai bune experiențe cu un grad mare de generalitate și practici** ale specialiștilor din toată lumea. Standardele oferă o bună structurare a informațiilor existente despre securitate și constituie ghiduri explicite de bune practici privind construirea și utilizarea SMSI.

O altă justificare ar fi **simplitatea și transparența** oferire de standarde, două cerințe imperative ale SI/SC, care corespund *principiului universal KISS: Keep It Simple, Stupid*. Mai simplu – este mai bine. Bunele practici și recomandările stabilite în standardele

de bune practici permit combaterea complexității. Utilizarea lor sugerează că nu trebuie să „născocești" nimic. Trebuie doar să urmezi îndeaproape bunele practici. Totodată, dacă SMSI este sau pare a fi prea vast, prea complex – se poate urmări dezvoltarea sa eșalonată, în acord cu **regula universală Pareto 20/80**: *este suficient să rezolvăm 20% dintre cele mai prioritare probleme pentru a atinge 80% din efectele preconizate*. Acest lucru este confirmat de abordarea SI/SC bazată pe riscuri, cu prioritizarea celor mai valorase resurse informaționale, ce au impact semnificativ asupra afacerii, cu identificarea, analiza, evaluarea și tratarea riscurilor majore ce amenință SC.

Foarte succint, implementarea SMSI în baza standardelor de bune practici **oferă numeroase beneficii pentru organizațiile și persoanele interesate** (entități):

- Ține organizația la curent cu toate informațiile actuale în domeniu;
- Introduce în organizație o metodă sistematică de control a confidențialității, integrității și accesibilități informației, un mediu unic ce conține toate mecanismele necesare pentru autocorectare și îmbunătățire continuă;
- Contribuie la păstrarea unui nivel bun de competitivitate pe piață, îmbunătățește credibilitatea și consolidează încrederea clienților;
- Contribuie la respectarea cerințelor legale privind securitatea informației;
- Oferă posibilitatea de îmbunătățire continuă prin audituri regulate;
- Asigură continuitatea afacerii, reduce costurile de asigurare și altele.

REZULTATE ȘI DISCUȚII

Cu toate că statisticele demonstrează că oamenii constituie cea mai slabă verigă în securitatea cibernetică, tot oamenii constituie și cel mai puternic remediu. Într-adevăr, oamenii pot provoca sau permite incidentele cibernetice din cauza lipsei de conștientizare sau a neglijenței lor, pregătirii slabe etc. Dar un personal sistematic instruit și împuternicit să acționeze poate spori cu mult siguranță împotriva amenințărilor cibernetice. Ei pot detecta și raporta activități suspecte, pot urma politicile și procedurile de securitate și pot folosi bunul simț și gândirea critică atunci când se confruntă cu situații critice. Ceea ce demonstrează elocvent schimbul accentului de pe componenta tehnică-tehnologică a SC pe cea umană, pe management, conștientizare, formare continuă, etc.

CONCLUZII

Adoptarea unor politici, standarde și practici robuste de SI/SC devine vitală pentru protejarea integrității, confidențialității și disponibilității informației într-o lume în care datele și informațiile sensibile sunt expuse din ce în ce mai mult riscului de furt, modificare sau distrugere ilicită.

Importanța SI/SC și a standardului ISO/IEC 27032 sunt justificate de impactul pe care atacurile cibernetice îl pot avea asupra indivizilor, entităților și societății în ansamblu, dacă acestea reușesc. Securitatea cibernetică conform familiei de standarde ISO27k, în special a standardului ISO/IEC 27032:2023, reprezintă o armă puter-

nică pentru gestionarea riscurilor cibernetice și protejarea infrastructurii digitale de amenințările curente și viitoare. Investiția în SI/SC și în conformitatea cu standardele internaționale în acest domeniu sunt cruciale pentru asigurarea unui mediu online sigur și pentru promovarea încrederii în utilizarea tehnologiei digitale în continuare. Însă *conformitatea cu reglementările, politicile, standardele respective nu garantează securitatea.* Inclusiv și pentru că acestea nu sunt/nu pot fi perfecte într-un mediu în continuă și bulversantă schimbare.

Respectarea principiilor sistemice ISO/IEC 27001:2022, aplicarea controalelor ISO/IEC 27002:2022 și ghidarea conform ISO/IEC 27032:2023 oferă *o abordare sistematică pentru construirea unui mediu digital mai sigur și mai rezistent în ciberspațiul global*. Sarcina familiei ISO27k și ISO/IEC 270032:2023, în special, rezumă în furnizarea unui set de ghiduri și recomandări pentru a asigura interacțiunea diferitelor tipuri de securități într-un mediu virtual unic din spațiul cibernetic. Ca atare, ISO/IEC 27032:2023 oferă linii directoare pentru îmbunătățirea SC în cadrul diferitelor entități prin dezvoltarea unui cadru de securitate bazat pe *managementul riscului în cadrul unor sisteme manageriale,* acoperind în special *securitatea informațiilor, securitatea rețelelor, securitatea pe Internet și Web, protecția infrastructurilor informaționale*.

Cu toate că controalele furnizate conform ISO 27032:2023 sunt controale preponderent tehnice *(e.g. securitatea rețelei, protecția serverului, protecția utilizatorului etc.),* alinierea sa cu principiile standardelor sistemice de management (ISO/IEC 27001:2022) încurajează personalul și utilizatorii să fie conștienți și proactivi pentru a crește eficiența și a maximiza eficacitatea măsurilor de SC.

De asemenea, este de menționat că aplicabilitatea universală a suitei standardelor ISO27k, indiferent de tipul afacerii, mărimea entității, regiune, țară favorizează implementarea acestor standarde comparativ cu cele naționale precum NIST sau standarde proprietare/specifice precum Top CIS Controls (de la SANS, CIS), COBIT de la ISACA etc.

REFERINȚE

1. *19 Tech Experts Bust Common Cybersecurity Myths And Misconceptions.* Decembrie, 1, 2023. În: https://www.forbes.com/sites/forbestechcouncil/2023/12/01/19-tech-experts-bust-common-cybersecurity-myths-and-misconceptions/?sh=6ee7695263ff. Accesat [25.06.2024].
2. *Top 10 Common Cybersecurity Myths.* În: https://agio.com/myths-about-cybersecurity/#gref. Accesat [25.06.2024].
3. *Cybersecurity Myths v/s Facts:* Unraveling *The Truth.* În: https://www.wattlecorp.com/cybersecurity-myths-facts/. Accesat [21.06.2024].
4. 239 Cybersecurity Statistics (2023). În: https://www.packetlabs.net/posts/239-cybersecurity-statistics-2023/, Accesat [18.06.2024].
5. *Mituri și legende ISO/IEC 27000.* (cu referire la întreaga familie ISO/IEC 27k).

În: https://www.consultanta-certificare.ro/articole/mituri-legende-iso-iec-27000.html . Accesat [21.06.2024].

6. FLECK, A. *Cybercrime expected to skyrocket in coming years*. Dec 2, 2022. În: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/. Accesat [18.06.2024].
7. MILKOVICH, Devon. *15 Alarming Cyber Security Facts and Stats.* În: https://www.cybintsolutions.com/cyber-security-facts-stats/. Accesat [18.06.2024].
8. Verizon Reports. *DBIR 2023 data breach investigations report.* În: https://www.verizon.com/business/ resources/Tbf7/reports/2023-data-breach-investigations-report-dbir.pdf. Accesat [18.06.2024].