Școala Națională de Studii Politice și Administrative
Facultatea de Administrație Publică

SECURITATEA CIBERNETICĂ ÎN INSTITUȚIILE PUBLICE (BEST PRACTICES)

- lucrare de licență, Administrație Europeană -

Coordonator

Conf. Univ. Dr. Cătălin VRABIE

Absolvent

Băjan Mihai Daniel

București
2024

Instrucțiuni de redactare (A se citi cu atenție!!)

1. Introduceți titlul lucrării în zona aferentă acestuia – nu modificați mărimea sau tipul fontului;
2. Sub titlul lucrării alegeți dacă aceasta este de licență sau de disertație;
3. Introduceți specializarea sau masteratul absolvit în zona aferentă acestuia de pe prima pagină a lucrării;
4. Introduceți numele dvs. complet în zona aferentă acestuia (sub Absolvent (ă));
5. Introduceți anul în care este susținută lucrarea sub București;

NB: Asigurați-vă că ați șters parantezele pătrate din pagina de gardă și cuprins.

6. Trimiteți profesorului coordonator lucrarea doar în format **Microsoft Word** – alte formate nu vor fi procesate;
7. **Nu ștergeți declarația anti-plagiat și nici instrucțiunile** – acestea trebuie să rămână pe lucrare atât în forma tipărită cât și în cea electronică;
8. **Semnați declarația anti-plagiat;**
9. **Cuprinsul este orientativ** – numărul de capitole / subcapitole poate varia de la lucrare la lucrare. **Introducerea, Contextul, Concluziile / Discuțiile și Referințele bibliografice sunt însă obligatorii;**
10. **Este obligatorie folosirea template**-ului. Abaterea de la acesta va cauza întârzieri în depunerea la timp a lucrării.

NB. Lucrările vor fi publicate în extenso pe pagina oficială a hub-ului Smart-EDU, secțiunea Smart Cities and Regional Development: https://scrd.eu/index.php/spr/index.

ATENȚIE: Lucrarea trebuie să fie un produs intelectual propriu. Cazurile de plagiat vor fi analizate în conformitate cu legislația în vigoare.

Declarație anti-plagiat
1. Cunosc că plagiatul este o formă de furt intelectual și declar pe proprie răspundere că această lucrare este rezultatul propriului meu efort intelectual și creativ și că am citat corect și complet toate informațiile preluate din alte surse bibliografice (de ex: cărți, articole, clipuri audio-video, secțiuni de text și sau imagini / grafice). **2. Declar că nu am permis și nu voi permite nimănui să preia secțiuni din prezenta lucrare pretinzând că este rezultatul propriei sale creații.** **3. Sunt de acord cu publicarea on-line *in extenso* a acestei lucrări și verificarea conținutului său în vederea prevenirii cazurilor de plagiat.** **Numele și prenumele: Băjan Mihai** **Data și semnătura: 6.11.2023**

Cuprins

Abstract

Lucrarea de față are ca scop analizarea, detalierea și explicarea modalităților de operarea în ceea ce privește gestionarea datelor și transmiterea acestora în cadrul instituțiilor publice. Din perspectiva obiectivelor abordate, se vizează înțelegerea nivelul curent de utilizare a tehnologiei în acest tip de instituții făcându-se o paralelă între organizațiile autohtone și cele la nivel European. Atenția urmează să fie pusă pe modalitățile în care informațiile sunt protejate prin diferite modalități de criptare și stocarea acestora.

Lucrarea este bazată pe analizarea studiilor și cercetărilor publicate în ultimii ani ce au ca obiect principal securitatea datelor, conceptele ce stau la baza sunt securizarea datelor prin utilizarea diferitelor metode de criptare și conștientizarea asupra nivelului de expunere la atacuri cibernetice. Prezenta lucrarea dorește să utilizeze o abordare de tip calitativ în ceea ce privește identificarea, integrarea și diseminarea informațiilor științifice disponibile în prezent pentru a putea genera o serie de recomandări.

De asemenea, studiul de caz selectat dorește creșterea gradului de conștientizare asupra expunerii ce vine la pachet cu responsabilitatea gestionării informațiilor în format digital de către instituțiile publice. Acesta dorește a trage un semnal de alarma în ceea ce privește un fenomen din ce în ce mai întâlnit în zilele noastre prin prisma multiplelor atacuri cibernetice identificate, cu atât mai mult cu cât procesul de digitalizare este un deziderat la nivel european și nu numai.

Se dorește a genera reacții în rândul specialiștilor în zona de securitatea a datelor ce activează în instituții publice, a managementului acestor organizații și nu în ultimul rând pentru cei ce pot legifera și proceduriza fenomenului și minimizarea riscului de pierdere sau divulgarea de date confidențiale în mediul public. Plus valoarea adusă de această lucrare vine prin prisma nivelului de transparență adus, gradul ridicat de structurarea și centralizarea multiplelor informații disponibile în prezent.

Cuvinte cheie: vulnerbilități, atacuri cibernetice, protejare date, criptare date, securitate.

Introducere

Privind în perspectivă importanță pe care informația o poate avea și a faptului că cine o deține poate influența sau controla ce urmează să se întâmple, putem înțelege importanța subiectului. Practic, încă din cele mai vechi timpuri, s-a ajuns la concluzia că pentru a avea un avantaj competitiv ai nevoie de informație. Fie că vorbim de conflicte armate, fie că vorbim de business sau de zona administrativă în cazul nostru, omenirea a început un proces de digitalizare accelerat, o cursă ce este sub cronometru în care viteza este esențială.

În ceea ce privește latura administrativă trebuie menționat că istoria a consemnat diverse forme de organizare publică încă din vremurile antice, având drept scop organizarea societății și îmbunătățirea ordinei și bunăstării publice.

Cum evoluția este inevitabilă, pasul firesc în ceea ce privește acest domeniu a fost îmbunătățirea accesul la informație și accelerarea nivelului de procesare. Astfel, un număr mai ridicat de cetățeni pot avea acces la diferite servicii și în speță responsabilitatea gestionării informațiilor acestora, cade pe umerii procesatorului de date, administrația publică. Printr-un exercițiu de imaginație, putem cu ușurință să proiectăm care ar fi consecințele dacă toate aceste date ar ajunge în mâinile unor persoane sau organizații cu intenții nu tocmai onorabile. Ce este sigur, este faptul că nu este un scenariu dezirabil, însă este un scenariu ce s-a întâmplat de nenumărate atât la nivel național, cât și internațional și cu siguranță se va mai întâmpla dacă nu învățăm din greșelile din trecut.

Pentru a-l cita pe Winston Churchill, „cei ce nu-și cunosc istoria sunt condamnați să o repete”. Astfel, studiul de față dorește să prezinte istoria, riscurile și modalități de îmbunătățirea a securității cibernetice în mediul public, subliniind importanța protejării datelor digitale. În ceea ce privește sursele informațiilor prezentate, s-au utilizat lucrări ale unor experți la nivel național și internațional.

Analizând în perspectivă lucrarea de față, putem sublinia faptul că în prima parte a acestei cercetări atenția a fost îndreptată către istoria conceptului de securitate cibernetică și evoluția acestui fenomen în zona de administrație publică.

Acest lucru a fost posibil compilând informații prezentate în diferite cercetări sau analize, informații de natura publică prezentate de o parte dintre aceste instituții ce sunt și subiect de studiu și nu în ultimul rând din publicații științifice. În a doua parte a acestei lucrări, s-a migrat către înțelegerea riscurilor unor potențiale atacuri cibernetice și care sunt cele mai uzitate breșe de securitate, iar, capitolul final a fost alocat studiului de caz pe o situație concretă a unui atac informatic asupra unei instituții publice pentru a demonstra care sunt consecințele.

Context

Lucrarea de față a luat naștere în contextul creșterii exponențiale a puterii de calcul, a accesibilității tehnologiei în zilele noastre, și nu în ultimul rând din cauză riscurilor din ce în ce mai ridicate ce apar din dorința de a digitaliza procesele administrative și nu numai. Crescând nivelul de digitalizare inevitabil ne expunem la anumite riscuri, iar, acele riscuri trebuie conștientizate și asumate. Așadar, utilitatea acestei lucruri și plus valoare pe care o aduce vine prin centralizarea si coroborarea de informații teoretice cu exemple concrete de practici (atât dezirabile, cât și eșecuri).

Capitolul 1. Rolul securității cibernetice în Administrația Publica / Europeană.

1.1. Istoria conceptului de Administrație Publică

În ceea ce privește administrația publică aceasta are rădăcini adânci în istorie, începând încă din cele mai vechi vremuri. Conform lui Heady Ferrelconceptul de administrație publică este identificat încă din primele societățile antice, precum cea a sumerienilor, babilonienilor și egiptenilor, care aveau sisteme organizate pentru administrarea justiției, colectarea taxelor și menținerea ordinii publice [1].

În Grecia Antică, cetățenii aveau un rol activ în administrarea afacerilor publice prin intermediul adunărilor și deliberărilor. Deși informațiile disponibile sunt relativ puține din perioada antichității, „marile proiecte dezvoltate de către aceste civilizații foarte dezvoltate nu puteau fi realizate în absența unei administrații publice extrem de bine alcătuite” [2].

Când facem referire la aceste proiecte ne putem uita inclusiv la cele „Șapte minuni ale lumii” și a modului în care muncitorii și întreaga infrastructură din spate necesita o foarte bună organizare din partea autorităților. Cunoștințele noastre despre Europa sunt ceva mai vaste, astfel avem informații referitor la Imperiul Roman si despre evoluția statelor europene din feudalism până la forma actuală.

În perioada Evului Mediu, puterea monarhilor a crescut, iar administrația a fost utilizată pentru a consolida controlul asupra teritoriilor. În această perioadă, s-au dezvoltat primele forme de birocrație, iar funcționarii au devenit tot mai specializați în îndeplinirea sarcinilor administrative. Odată cu Renașterea, gânditorii au început să pună accent pe idei precum guvernarea rațională și drepturile omului, influențând evoluția ulterioară a administrației.

Iluminismul a adus idei precum separarea puterilor și importanța transparenței în administrație. În secolele XVIII și XIX, cu Revoluția Franceză și Revoluția Industrială, s-au produs schimbări semnificative în structurile administrative. Ideile lui Max Weber despre birocrație au influențat organizarea și funcționarea administrațiilor publice din întreaga lume [3].

În secolul XX, administrația publică a fost modelată de schimbările sociale, economice și politice, precum mișcările pentru drepturile civile, tehnologia informației și globalizarea. Organizațiile internaționale au devenit mai implicate în problemele de administrare globală, iar rolul statului în economie și în oferirea serviciilor publice a fost reevaluat [4].

În prezent, administrația publică se confruntă cu provocări complexe, cum ar fi tehnologia avansată, schimbările climatice și gestionarea pandemiilor. Concepte precum guvernarea deschisă și participarea cetățenilor sunt tot mai importante. Utilizarea tehnologiei informației și comunicării a revoluționat procesele administrative, asigurând o mai mare eficiență și transparență [5].

Este imperativ necesar în a înțelege care au fost principalele etape în dezvoltarea administrației publice în România. Din această perspectivă există o anumită dilemă/semn de întrebare între specialiști în ceea ce privește linia temporară pe care o avem în analiza vs. tipului de organizare a statului avut în studiu.

Alegând o abordare generică am decis să ne focusăm pe istoria conceptului din perspectiva istoriei dreptului românesc și avem la bază opiniile exprimate de Vladimir Hanga (Istoria Dreptului Românesc) și de Dumitru Firoiu (Istoria Statului și Dreptului Românesc) care împart această zonă în 6 etape:

Administrația monarhiei dacice ce vizează perioada de la formarea statului dac și culminează cu perioada lui Burebista și Decebal, până la cucerirea Daciei de romani în anul 106 d. Hr.

Administrația și dualismul juridic și se concentrează pe Dacia ca provincie a Imperiului Roman (106-274 d. Hr).

Administrația feudală cuprinde retragerea aureliană și înființarea statelor române centralizate și perioada monarhiei centralizate până la revoluțiile din 1821.

Administrația modernă capitalistă care cuprinde perioada dintre revoluțiile burgheze 1821 și 1848, până în 1947 și stabilirea noilor instituții capitaliste.

Administrația socialistă care cuprinde perioada 23 august 1944 și 22 decembrie 1989.

Administrația de tranziție de după 1989 până la integrarea României în Uniunea Europeană în 2007.

Din această perspectivă, istoria notează faptul înregistrări locale debutează încă din perioada Principatelor române fiind sub dominație rusă și ulterior momentul proclamării independenței față de Imperiul Otoman și înființarea României din zilele noastre [6].

1.2. Procesul de digitalizare al Administrației Publice / Europene

Având o înțelegere mai aprofundată în ceea ce înseamnă termenul de Administrație Publică și cum s-a manifestat atât local, cât și la nivelul mondial, putem avansa în discuție și să ne concentrăm pe un subiect cât de se poate de actual: importanța tehnologiei și impactul acesteia în toate domeniile.

La nivel global, aportul tehnologiei a fost unul masiv în ultimii 20 de ani, iar, prin prisma devenirii din ce în ce mai accesibile a mijloacelor de comunicare și a popularizării internetului, în prezent putem afirma ca intrăm într-o nouă era. Schimbare și/sau dezvoltarea este inevitabilă indiferent de domeniu, iar, cu atât mai mult zona tehnologiei. Practic, putem privi în istorie și observă diferite momente importante cheie ce au marcat omenirea printre care revoluția industrializării din perioada 1760-1840 pornită concomitent în Marea Britanie și în Statele Unite ale Americii.

Următoarea etapă consemnată de istorie a fost a doua revoluție a industrializării între anii 1870 – 1940 si s-a finalizat cu începutul Primului Război Mondial. Această etapă a avut ca focus standardizarea și industrializarea și nu în ultimul rând rafinarea tehnologiilor introduse anterior.

De asemenea, perioada în cauză a fost notabilă pentru introducerea unor concepte/invenții importante precum utilizarea energiei electrice (invenția becurilor incandescente de către Thomas Edison 1879-1880), apariția telefoanelor (Graham Bell 1876) și motorul cu ardere interna (1872). Această etapă a fost una importantă pentru că a generat un val important de idei, schimbări de concepte (linii de producție, nevoia de un management mai eficient, etc) și mai important a marcat începutul globalizării prin accesul la informație mult mai facil și rapid.

Următoarea etapă a fost revoluția digitală din anul 1960 ce a fost determinată de schimbarea de la tehnologia analogică către digitală și electronică, având ca piese centrale tranzistorii și circuitele integrate. Din acest punct au fost derivate tehnologii precum microprocesoare, computere, telefoane mobile și nu în ultimul rând internetul. Printre fundamentele acestei etape se regăsesc colectarea, transmiterea și utilizarea datelor pentru a aduce plus valoarea [7].

Etapele menționate anterior și-au pus amprenta pe toate domeniile ce ne înconjoară, iar, Administrația Publică nu face excepție. Acest concept ce a fost și este în slujba cetățenilor, a fost impactat inevitabil. Acum, ar fi greu de spus aceste schimbări au fost efectuate în același timp, sau într-un ritm ceva mai lent comparativ cu alte industrii, însă, ce este important este faptul că schimbarea este inevitabilă.

Administrația publică a trecut în istoria ei prin multiple schimbări și transformări, pe o parte pentru a se adapta la cerințele societății la momentul respectiv și pe alta pentru că industria și tehnologia au fost și încă sunt într-o continuă dinamică. Din perspectivă organizatorică, la începuturile ei, administrația publică se baza preponderent pe zona de documente în format fizic și interacțiuni.

Ulterior, pe măsură ce avansul tehnologic a luat amploare zona administrativă a migrat către o zona de inovație și eficienței, având acces la diferite programe software pentru gestionarea datelor, automatizarea proceselor și creșterea eficienței serviciilor publice. Automat, această etapă a venit la pachet cu creșterea eficienței prin prisma accesului la informație, modalități de comunicare facile cu cetățenii și nu în ultimul rând cu zona de transparență.

Tehnologia a avut un impact semnificativ asupra dezvoltării conceptului de administrație publică la nivel global, generând o multitudine de schimbări în modul în care guvernele furnizează servicii, iau decizii și interacționează cu cetățenii. Din această perspectivă, principalele zone pe care tehnologia le-a influențat în administrația publică sunt: eficiență și transparență, serviciile electronice și de guvernare electronică (e-guvernare), big data si analiza predictivă, automatizări și inteligența artificial, participarea cetățenilor, lucru de la distanta și mobilitate și nu în ultimul rând securitatea cibernetică ți protecția datelor.

Din perspectiva eficienței și transparenței sistemele informatice și platformele au reușit să crească semnificativ eficiența proceselor administrative, reducând birocrația și scurtând timpul necesar pentru luarea deciziilor. La polul opus aveam un alt beneficiu semnificativ adus de tehnologie și anume gestionarea mult mai eficiente a resurselor disponibile și implicit a bugetelor.

Conceptul de „e-guvernare”, așa cum a fost definit de către Cătălin Vrabie în lucrarea „Elemente de E-guvernare” poate să fie definit în două modalități: fie ca „utilizarea tehnologiei informației de către agențiile guvernamentale în relațiile cu cetățenii, întreprinderile și alte corpuri guvernamentale” sau ca fiind „folosirea tehnologiei informației, în particular a Internetului, pentru a livra servicii publice într-o manieră mult mai convenabilă, eficientă și orientată spre client” [8].

Zona de e-guvernare a venit la pachet cu dezvoltarea serviciilor si permiterea cetățenilor să interacționeze cu guvernul prin intermediul internetului. Acesta include acces la servicii precum plata taxelor online, depunerea și generarea de documente electronice și accesul la informații de ordin administrativ.

Big data și analiză predictivă are în vedere colectarea și analizarea unor cantități masive de date ce au permis administrațiilor publice să obțină informații în detaliu cu privire la nevoile cetățenilor, să identifice tendințe și să ia decizii informate [9]. Componenta de analiza predictivă are în vedere prevenirea și anticiparea problemelor înainte ca acestea sa devină critice.

Inteligenta artificiala este în prezent un subiect pe buzele tuturor indiferent de domeniul sau industria în care activează. Utilizarea acesteia în administrația publică a dus la creșterea eficienței în procese repetitive și la reducerea erorilor umane. Sistemele semi-automatizate de tip chatbot (este un sistem automatizat de comunicare ce imită o interacțiune umană, iar, de cele mai multe ori au în spate un algoritm de tip arbore decizional), asistenta vocală și alte aplicații similare sunt utilizate în a oferi suport cetățenilor, și pentru a răspunde într-un timp cât mai scurt întrebărilor acestora [10].

Participarea cetățenilor a fost facilitată în special prin utilizarea tehnologiei la masă largă, iar, aceștia au putut lua parte la procesul decizional. Din această categorie putem enumera platforme online, rețele sociale și instrumente de feedback ce permit cetățenilor să-și exprime opiniile, să participe la dezbateri și să contribuie la procesul de luare a deciziilor.

Sistem automatizat de comunicare ce imită o interacțiune umană, iar, de cele mai multe ori au în spate un algoritm de tip arbore decizional. O alta zona integrată a tot ce înseamnă tehnologizarea ce s-a resimțit inclusiv în administrație publică este lucru la distanță și creșterea mobilității angajaților instituțiilor. Prin acces la informații de pe dispozitive mobile, multe roluri/poziții s-au transformat și au început să redefinească standardele și activitățile desfășurate.

Toate aceste schimbări au venit la pachet cu o serie notabilă de provocări, iar, prin prisma acestor provocări, la nivel european au fost necesare o serie de modificări legislative. În 2016, Parlamentul European a adoptat Directiva NIS (NIS – acronim din engleză pentru Network and Information Systems), prima piesă din pachetul legislativ pentru zona de securitate cibernetică. Această directivă impunea statelor membre să consolideze apărarea infrastructurii de natura critică cum ar fi energie, transport, utilități, servicii bancare și sectorul medical [11].

Operatorii acestei infrastructuri critice trebuie să notifice autoritățile naționale cu privire la incidentele cibernetice grave, iar statele membre trebuie să împărtășească informații despre riscurile și amenințările în curs [12].

În 2021, Comisia Europeană a generat o serie de actualizări ale acestei directive si a intitulat programul NIS2. Aceste actualizări au vizat extinderea scopului inițial în așa fel încât să includă spațiu, servicii de curierat, alimentație, managementul deșeurilor, administrația publică și servicii digital precum rețele sociale sau centre de date.

În conformitate cu NIS 1 și 2, autoritățile naționale eliberează certificate care confirmă că un produs a trecut testele de securitate proporționale cu nivelul de risc al produsului: de bază, substanțial sau ridicat. Toate țările UE sunt obligate să recunoască certificatul, facilitând comerțul transfrontalier și economisind afacerilor timp și bani pe mai multe certificări, potrivit Comisiei Europene [13].

Directivele NIS de securitate cibernetică conțin și alte defecte semnificative. Acestea fac distincție între sectoarele critice și cele necritice, despre care contestatarii avertizează că pot să creează o distincție falsă, deoarece este dificil până la imposibil să se separe și să clasifice pericolele în lumea digitală. Dacă totul este conectat, totul devine infrastructură critică, notează Ot van Daalen, cercetător în domeniul securității cibernetice la Universitatea din Amsterdam.

O cameră vulnerabilă ar putea fi folosită pentru a executa un atac DDoS împotriva unei companii de energie, sau un router piratat ar putea fi folosit pentru a accesa o bază de date critică de asistență medicală [14].

Europa încearcă să minimizeze aceste inadvertențe sau chiar să le elimine prin Cyber Resiliance Act (Legea privind reziliența cibernertică), în Septembrie 2022 este elaborată o propunere ce stabilește un set comun de standarde cibernetice pentru dispozitive și servicii contactabile ce nu erau acoperite până în prezent de precedentele standarde. Produsele care încalcă regulamentul s-ar confrunta cu amenzi de până la 15 milioane de euro sau 2,5% din cifra de afaceri la nivel mondial, oricare dintre acestea este mai mare. Acest act vine cu o serie de clasificări printre care „standard”, „clasa I” sau „clasa II”.

Produsele de clasa I prezintă riscuri minime de securitate. Producătorii lor trebuie fie să urmeze standarde specifice, fie să finalizeze un proces de certificare terță parte. Acestea includ browsere, manageri de parole, software de identitate și acces, routere și modemuri și aplicații pentru dispozitive mobile.

Produsele de clasa II prezintă cel mai mare risc de securitate și trebuie să primească certificare de la terți înainte de a fi puse pe piață. Acestea includ sisteme de operare software, infrastructură publică și emitenți de certificate digitale, routere și comutatoare industriale, dispozitive industriale pentru internetul obiectelor, senzori de roboți și contoare inteligente.

Aproximativ 90% dintre produsele digitale ar intra în această categorie cu risc ridicat, inclusiv software-ul de editare foto și jocurile video care nu prezintă pericole cibernetice real [15].

Cyber Resiliance Act nu s-ar aplica dispozitivelor deja acoperite de legislația dedicată, cum ar fi dispozitivele medicale și automobile. De asemenea, ar fi impuse reguli suplimentare pentru sistemele de inteligență artificială care ar fi clasificate drept risc ridicat într-o lege separată privind IA, care este în curs de negociere [16].

Legislația cibernetică ar intra în vigoare în două etape. În termen de 12 luni de la adoptare, producătorii ar trebui să raporteze încălcările și vulnerabilitățile securității cibernetice, iar în 24 de luni, statele membre și întreprinderile afectate ar trebui să se conformeze [17].

Alți critici corporativi se tem că Cyber Resilience Act ar putea încetini sau chiar opri lansarea noilor tehnologii și servicii esențiale. „Afacerile ar trebui să aștepte certificarea înainte de a adopta securitatea produsului", spune Alexandre Roure de la Computer & Communications Industry Association [18] .

1.3. Tipuri de date si modalități de protejare ale acestor date

Prin prisma perioadei în care trăim, fiind înconjurați de tehnologie și internet în aproape fiecare minut din viețile noastre, am fost expuși atât la efecte pozitive, cât și negative. Multiplele avansuri tehnologice prin care am trecut au permis, de asemenea, creșterea gradului de colectare și procesare de date care, în trecut, de cele mai multe ori, erau date uitării. Cum astăzi capacitatea de stocare disponibilă este aproape nelimitată, în egală măsură capacitatea de analiză a crescut semnificativ.

Ce este cu adevărat impresionant, este faptul că fiecare informație luată individual din tot ceea ce ne reprezintă (viață personală, business, interacțiuni cu zona de administrație publică, etc) nu înseamnă musai ceva, însă, privind într-un context mai general toate aceste informații pot duce la elaborarea de profile de personalitate, iar, implicit cresc gradul de vulnerabilitate.

Dreptul la viață privată și dreptul la protecția datelor cu caracter personal au devenit două dintre cele mai importante drepturi fundamentale ale societății moderne. Dezvoltările din domeniul vieții private necesită un cadru legal și politic inovativ care poate asigura că implicațiile tehnologice sunt corect înțelese și, prin urmare, reglementate corespunzător.

Pentru a avea o înțelegere mai aprofundată referitor la care a fost evoluția conceptului de date de-a lungul timpului, este necesar să ne înțelegem de unde am plecat și unde am ajuns în prezent. Astfel, putem analiza ce schimbări trebuie efectuate pentru a îmbunătății situația.

Încă din cele mai vechi timpuri s-a constant că cel ce posedă cunoștințe sau informații deține puterea. Dovadă că primele tehnici de a ascunde sau cripta informații datează din perioada popoarelor egiptene, a celor grecești și a celor romane, cu scopul de a proteja informațiile sensibile din a fi citite și înțelese de persoane nedorite.

Egiptenii se foloseau de un sistem bazat pe hieroglife pentru a face înscrieri pe diferite medii de scriere de la lemn, piatra, etc. De cele mai multe ori, scrierea era una destul de simplă și directă utilizând caractere sub formă de imagini ce ulterior puteau fi citite ca imagini, obiecte sau sunete [19].

Fig. 1. Hieroglife egiptene.
Sursa: https://www.britannica.com/topic/hieroglyphic-writing.

În Grecia antică, spartanii utilizau bucăți lungi de piele pe care le înfășurau în jurul unor bețe (schitală). Înfășurate pe aceste bețe, informațiile nu aveau sens, însă odată ce erau desfășurate ele puteau fi descifrate datorită diametrului bățului în jurul căreia erau înfășurate.

Fig. 2. Schitala.
Sursa: https://ro.wikipedia.org/wiki/Schital%C4%83.

În Roma, algoritmul de criptare al lui Julius Caesar a fost și este utilizat ca o modalitate de criptare a informațiilor bazată pe o substituire simplă a literelor. Astfel, fiecare literă din alfabet era schimbată cu o alta, existând un număr exact de poziții (variind între 0 si 24), în urma căreia substituția era realizată [20].

Metoda în cauză, deși este rapidă și eficientă din perspectiva rezultatului, nu este suficient de complexă fiind expusă la a fi spartă. Cu toate acestea, ulterior, au fost dezvoltate alte variații alei aceste metode printre care cea mai cunoscută ar fi ceea elaborată Giovan Battista Bellaso purtând numele Cifrul Vigenère (pe scurt, aceasta variație utilizează doua chei asimetrice) [21].

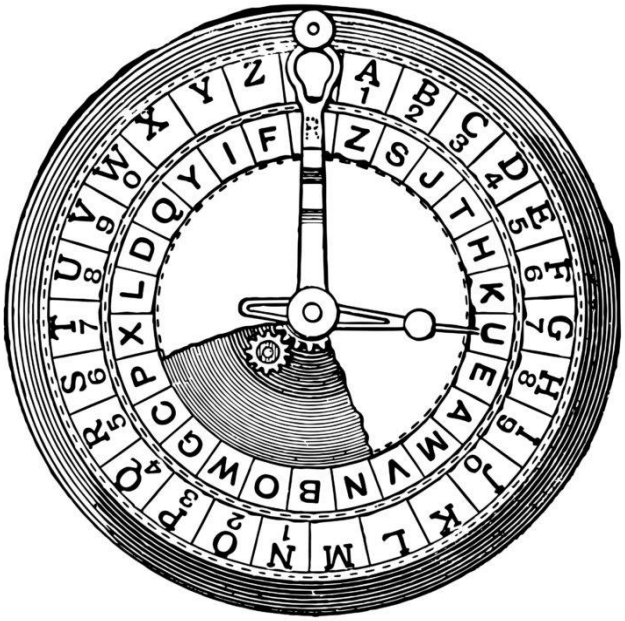


Fig. 3. Cifrul lui Caesar.
Sursa: https://gkaccess.com/support/information-technology-wiki/caesar-cipher/.

În secolului al XV, a fost creat un alt sistem de criptare a informațiilor de către Leon Battista Alberti. Sistemul avea la bază două rânduri de litere și o parte mobilă. Acest disc a fost creat pentru a cripta și a decripta mesajele fie prin lăsarea părții mobile în aceeași poziție (astfel rezultând cifrul monalfabetic) fie prin deplasarea periodică a părții mobile (rezultând cifrul polialfabetic).

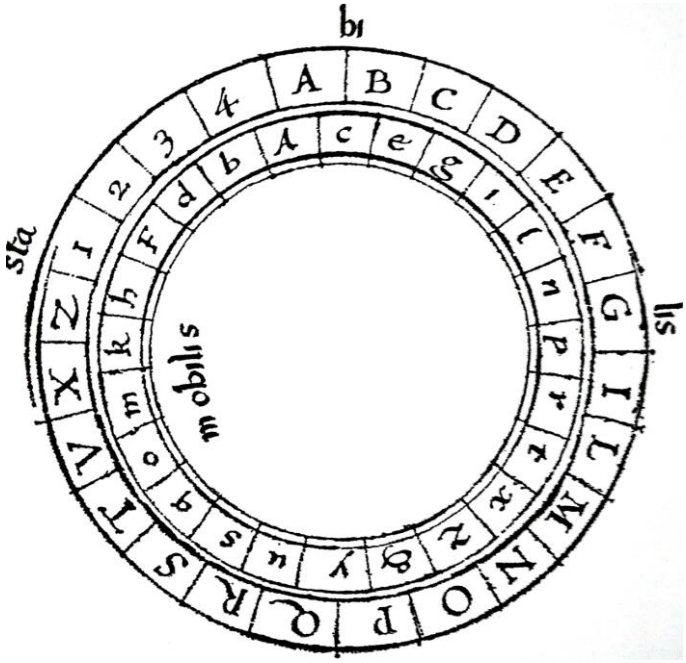
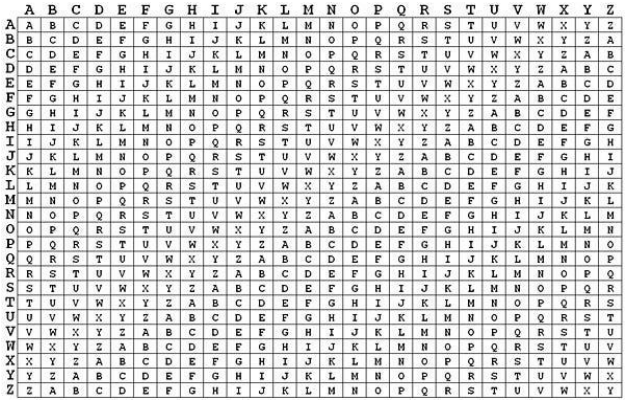


Fig. 4. Sistemul de criptare al lui Leon Battista Alberti.
Sursa: https://www.telsy.com/leon-battista-albertis-cipher-disk/.

În anul 1518, Johannes Trithemius a dezvoltat un alt sistem de codare numit „tabula recta” ce are la bază aceiași abordare polialfabetică prezentată anterior. Acesta avea forma unui pătrat și era format din mai multe alfabete ce erau decalate vs linie precedentă [22].



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fig. 5. Sistemul de criptare al lui Johannes Trithemius .
Sursa: https://cyberw1ng.medium.com/understanding-the-trithemius-cipher-a-comprehensive-guide-2023-8e2c705a0d15.

Avansând în timp ajungem în epoca modernă și inventarea telegrafului, împreună cu codul morse. În 1832, Samuel F. B. Morse, un ilustru profesor de pictură și sculptură în cadrul Universității New York, a început să fie interesat de ideea impulsurilor electrice și de aplicabilitatea acestora în zona de telecomunicații. Doi ani mai târziu acesta a dezvoltat un sistem ce era compus din puncte și linii fiind echivalentul literelor și numerelor, iar, în 1837 a patentat prima versiune a telegrafului. Ulterior, acest sistem a fost perfecționat cu ajutorului Alfred Vail și a suportului financiar obținut din partea guvernului Statelor Unite.

Din această perspectivă, prima demonstrație a utilității acestui dispozitiv a fost interconectarea a două orașe, Washington și Baltimore, aflate la aproximativ 60 de km depărtare. Deși inițial a fost gândit și proiectat pentru a gestiona traficul feroviar, telegraful a luat amploare și a început a fi utilizat la nivel global.

De-a lungul timpului, tehnologia a continuat a fi îmbunătățită atât funcțional (înlocuirea receptorului cu un sistem auditiv ce permitea operatorului să preia mesajul), cât și la nivel de concept prin dezvoltarea de transmisii duplex (utilizarea aceiași linii atât pentru transmisie și recepție simultan) [23].

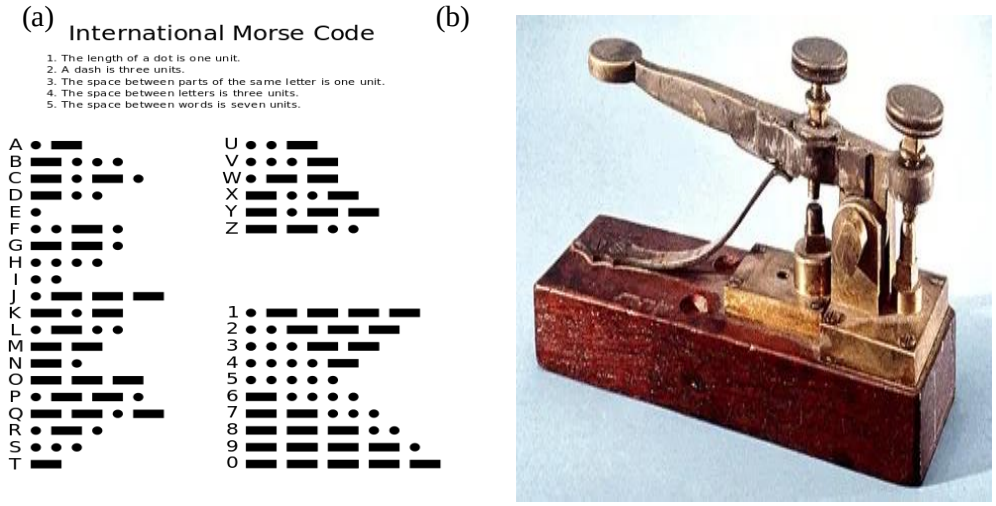


Fig. 6. (a) codul morse (versiunea internațională); (b) dispozitiv parte din sistem.
Sursa: https://www.britannica.com/technology/telegraph/Development-of-the-telegraph-industry.

Telegraful a marcat începutul comunicațiilor la nivel global și nu facem referire doar la componenta civilă sau comercială, ci și la utilizarea intensivă în cadrul comandamentelor militare.

Prin intermediul lui a fost posibil controlul permanent al acțiunilor militare și creșterea cantității de informație ce putea fi transmisă.

În timpul primului război mondial radioul a fost folosit ca mijloc de transmitere a informațiilor, astfel a crescut exponențial cantitatea de informație fapt ce a avut ca o consecință secundară creșterea interesului pentru criptanaliză. Acest lucru s-a datorat dorinței de a intercepta și a decripta mesajele trimise de către inamici pe frontul de luptă. La începutul anilor 1920 a fost dezvoltată o nouă metodă de criptografie ce avea ca scop protejarea mesajelor diplomatice.

Tehnica consta în utilizarea unor ,,blocuri cu o singură utilizare", așa cum a fost această metodă cunoscută. Blocurile erau formate din cifre aleatorii (grupate sub forma unor grupuri) ce mai apoi erau tipărite și legate într-o carte. Secretul acestei metode consta în utilizarea unică a fiecărei foi (după ce erau folosite acestea erau aruncate).

Chiar dacă metoda a fost dezvoltată în cel mai mare secret, ea a sfârșit prin a fi răspândită în întreaga lume în mai puțin de 15 ani. Chiar și în ziua de astăzi această tehnică de criptare este cunoscută ca fiind una din cele mai sigur metode criptografice și este folosită în continuare [24].

Așa cum deja s-a menționat, protejarea datelor prin diferite metode a jucat și o să joace un rol extrem de important pe multiple contexte cu implicații majore. Dovada stau nenumărate războaie sau bătălii ce au fost câștigate sau pierdute, în funcție din perspectiva cărei tabere privim lucrurile.

Ca urmarea a acestei necesități de protejarea a datelor, în timpul celui de-al doilea război mondial apare o nouă invenție ce are a scop criptare mesajelor și anume Enigma, elaborată de Arthur Scherbius. Acest dispozitiv stătea în spatele tuturor comunicațiilor esențiale pentru trupele armate germane și a fost decriptat prin prisma capturării unui dispozitiv și a unui caiet de coduri în data de 9 Mai 1941.

În ceea ce privește procesul de decriptare pentru dispozitiv echipa condusă de Alan Turing a reușit în a identifica o eroare de proiectare ce a condus la „spargerea" codului. Ulterior, dispozitivul a fost reproiectat, având în vedere eroarea identificată, și utilizată de aliați în război. Datorită acestui eveniment, se preconizează că al războiul a fost scurtat cu aproximativ 2 ani și că s-au salvat peste 14 milioane de vieți omenești [25].

Fig. 6. Enigma.
Sursa: https://edition.cnn.com/2011/09/29/world/europe/uk-enigma-machine-auction/index.html.

Trecând prin toate aceste exemple, putem afirma cu tărie că protejarea informațiilor din domeniul public a ajuns a fi un deziderat pentru toți cei implicați fie că vorbim de persoane private, corporații sau guverne.

Deși în prezent vorbim de o cu totul și cu totul altă dinamică atunci când ne raportăm la volumul de date disponibile, temerile și riscurile sunt aceleași, sau poate chiar mai ridicate prin prisma procesului de digitalizare.

Trebuie luat în considerare că trecerea din mediul fizic către mediul online a schimbat aproape în totalitate regulile jocului. Din această perspectivă, digitalizarea exponențială prin care trecem în prezent a dus la creșterea atacurilor cibernetice ce au ca scop accesarea neautorizată a informațiilor, furtul de identitate sau alterarea datelor. Aceste atacuri cibernetice pot avea consecințe multiple cu impact financiar sau moral, iar, resurse impresionante sunt alocate pentru implementarea de măsuri de protecție.

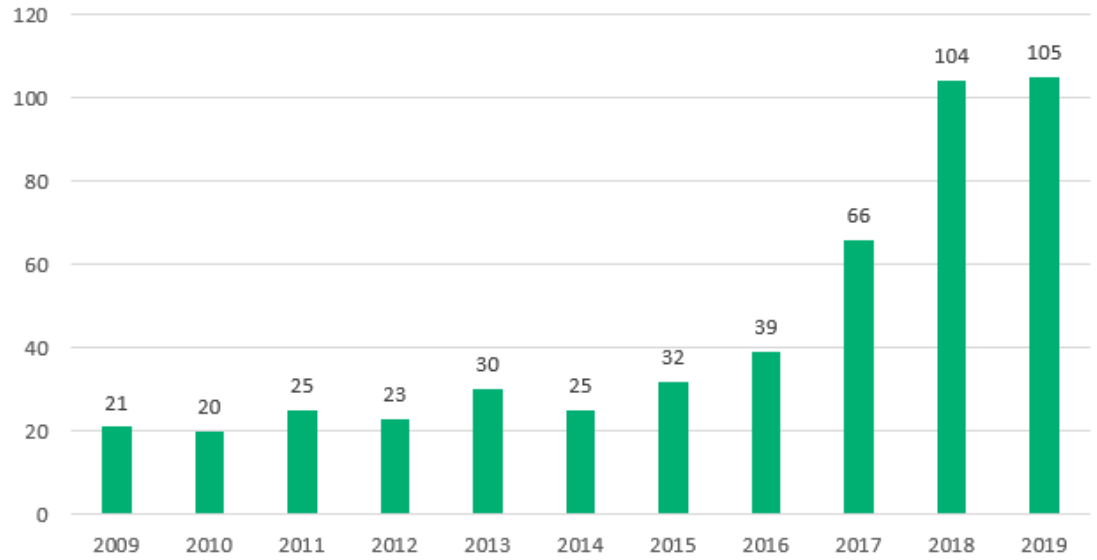


Fig. 7. Evoluția atacurilor cibernetice generatoare de pierderi mai mari de 1 mil de dolari.
Sursa: https://sectigostore.com/blog/42-cyber-attack-statistics-by-year-a-look-at-the-last-decade/.

De asemenea, deși nu este focusul acestei lucrări, inevitabil trebuie să luăm în considerare și latura juridică pe care gestionarea acestor date o ridică și implicit trebuie să avem în vedere zona de GDPR (General Data Protection Regulation) ce a fost elaborat și ulterior implementat de Uniunea Europeană [26].

Mai concret, acest regulament are în centrul său persona fizică și protejarea datelor cu caracter personal prin măsuri adecvate împotriva dezvăluirilor către terți și împotriva utilizării nelegale. Regulamentul GDPR are ca fundament conceptul de responsabilitate, iar, operatorul de date este responsabil în a implementa măsuri de securitate adecvate pentru protecția datelor și are obligația să demonstreze și să documenteze acest lucru.

Regulamentul GDPR are în spate o serie de principii:

- principiul legalității, echității și transparentei: presupune că datele cu caracter personal trebuie prelucrate conformitate cu legea și să se încadreze în temeiurile juridice de prelucrare stipulate în art. 6 iar, în caz contrar organizația poate fi amendată pentru prelucrare ilegală. De asemenea, acest principiu subliniază faptul că aceste date nu pot fi prelucrare în moduri incorecte ce ar putea prejudicia persoanele vizite. Transparența venind la pachet și impune ca încă de la început să fie prezenta modul în care organizația prelucrează aceste date;
- principiul limitării scopului: se rezumă la determinarea scopului prelucrării datelor într-o manieră explicită și legitimă. Practic, previne situația în care datele sunt colectate pentru un anumit obiectiv, iar, ulterior sunt procesate și în alte scopuri;
- principiul reducerii la minim a datelor: vizează colectarea minimului necesar de date în vederea atingerii scopurilor;

- principiul exactității: datele cu caracter personal trebuie să fie exacte, complete și actualizate, iar, organizațiile trebuie să depună eforturi în a verifica și aceste informații, în caz contrar șterse;
- principiul integrității și confidențialității: asigurarea protecției datelor de către operator împotrivă accesării neautorizate și împotriva pierderii, distrugerii sau a deteriorării accidentale;
- principiul responsabilității: operatorul este nu este doar responsabil pentru respectarea normelor GPDR, ci și trebuie să fie capabil să demonstreze că respectă aceste principii.

Trebuie ținut cont de faptul că acest regulament se răsfrânge pe întreg spectrul de interacțiuni pe care o organizație îl poate avea de la interacțiunea cu un client în cazul unei companii private sau cu un contribuabil în cazul unei instituții publice, până la diferite parteneriate pe care le-ar putea avea cu furnizori, clienți, colaboratori, etc.

Din această perspectivă fiecare parte implicată în diferitele interacțiuni trebuie să aibă în vedere complianța cu normele și procedurile regulamentul pentru protecția datelor. În acest context apare în literatura de specialitate terminologia de „acorduri între operator și persoana împuternicită". Toate aceste interacțiuni sunt supravegheate de autorități independente la nivelul fiecărui membru UE. În România ANSPDCP (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) este entitatea ce este responsabilă.

O altă latură foarte importantă, care impactează semnificativ zona de securitatea cibernetica în contextul global în care operam este partea de transferuri internaționale de date. Aceste transferuri de date ale cetățenilor europeni către alte state non-UE au fost luate sub analiza din perspectiva securității datelor. Deși, regulamentul nu interzice în mod expres transferurile de date, acesta prevede ca anumite garanții adiționale sunt necesare:
- clauze contractuale standard
- regulamente corporate [26].

Întorcându-ne la subiectul nostru suntem nevoiți să privim în perspectivă și să înțelegem că modul în care acționam zilnic prin tot ceea ce facem, chiar daca pare fără a avea o semnificație majora (pe moment cel puțin), lasă urme digitale și poate avea repercusiuni. Aici vorbim pe o parte de postura de utilizator final în care accesam website-uri, aplicații și platforme uzuale cum ar fi Meta (WhatsApp, Facebook, Instagram), TikTok, Snapchat sau fiecare site ce poate colecta si gestiona cookies, până la postura de organizații sau persoane ce pot avea foloase materiale sau morale pe urma informațiilor pe care pot colecta, prelucra și utiliza în scopuri alternative decât cele inițiale.

Pentru a prezenta câteva exemple de astfel de organizații nu putem să nu menționam cea mai mare amenda aplicata pentru nerespectarea normelor GDPR și anume 1.2 miliarde USD pe care Meta a fost obligată să o achite în 2023 pentru nerespectarea normelor de transfer internațional [27].

De asemenea, este necesar să menționăm și un exemplu mult mai aproape de latura administrativ publică în care activăm și anume campania electorală în care Partidul Republican din Statele Unite ale Americii l-a avut drept candidat pe Donald Trump în 2016. Acest exemplul este unul de o complexitate impresionantă prin prisma abordării utilizate de reprezentanții de campanie ai candidatului la președinție cu ajutorul Cambridge Analytica.

Fără a intra în prea multe detalii Cambridge Analytica a cumpărat, colectat și procesat date pentru a elabora modele predictive asupra tipului de utilizator și le-a transpus in diferite forme de conținut ce ulterior au fost răspândite pe rețele de socializare, având drept focus tipul de utilizatori în cauză. În tot acest timp a exista o bucla de feedback între rezultatele campaniilor online și nivelul de angajament (pe diferitele rețele sociale) astfel încât ROI (acronim din engleză pentru Return On Invest) să fie optim. Rezultatul final a fost unul impresionant: câștigarea cursei electorale în unul dintre cele mai importante și puternice state la nivel global [28].

1.4. Politici de securitate cibernetică

Vorbind de un grad ridicat de interconectabilitate prin prisma interacțiunilor cu tehnologia pe care le avem zilnic, putem afirma că ultimul deceniu au transformat mediul de afaceri global, cu progrese continue în toate domeniile de la lucrul în echipă, stocarea datelor în cloud și blockchain[1] la AI[2] și IoT[3].

Riscul cibernetic a trecut la un nivel superior, dincolo de deja „clasicele" breșe de securitate și scurgeri de date sensibile, ajungând la scheme sofisticate care pot perturba o întreagă companie sau industrie, gestionarea unui lanț logistic de aprovizionare sau chiar, la nivel guvernamental, pot afecta funcționarea unui stat. Pagubele se ridică la miliarde de euro și afectează companiile din orice sector de activitate și economiile naționale [29].

Într-un studiu publicat în 2019 de Marsh și Microsoft [30] ce a avut ca obiectiv evaluarea percepția asupra riscurile cibernetice și modul în care le putem analiza și gestiona, au reieșit următoarele:

- Nivelul de comprehensiune ale riscurilor atacurilor cibernetice a crescut. Prin prisma frecvenței și a severității incidentelor cu impact major asupra securității datelor, prioritățile organizațiilor s-au schimbat semnificativ în ultimii ani.
- Raportat la multitudine de variabile cu care o organizație se confruntă zilnic (economic, financiar, uman, legal, etc) riscul cibernetic ocupă locul întâi
- Majoritatea organizațiilor au luat în considerare sau urmează sa adopte tehnologii noi.

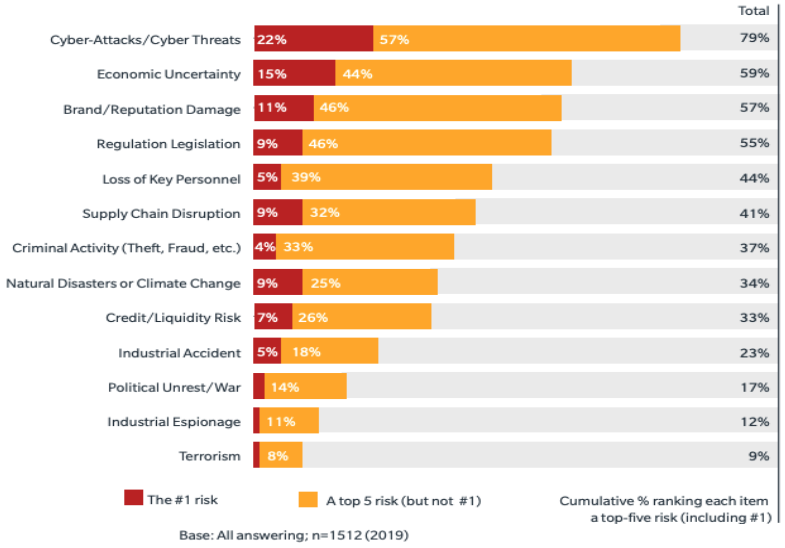


Fig. 8. Clasificarea percepție riscurilor de organizații.
Sursa: https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf.

Rolul administrațiilor publice deși este unul important în teorie, conform studiului, realitatea este că organizațiile consideră că reglementările și standardele de industrie impuse au un grad limitat de eficacitate în a gestiona riscul cibernetic – excepție făcând atacurile la nivel național.
Practic putem observa că 28% dintre companii se referă la reglementările sau legile guvernamentale (NIST[4], SOC2[5], ISO[6], etc) ca fiind foarte eficient în îmbunătățirea securității

[1] Blockchain - este o tehnologie de stocare și transmitere a informațiilor, care se bazează pe principiul distribuirii și securității.
[2] AI – acronim din engleză pentru Artificial Intelligence
[3] IoT – acronim din engleză pentru Internet of Things
[4] National Institute of Standards and Technology – Institutul Național de Standarde și Tehnologii
[5] System and Organization Controls – Controlul Sistemelor și al Organizației
[6] International Organization for Standardization – Organizația Internațională pentru Standardizare

cibernetice. Dintre acestea doar 37% dintre companii consideră standardele impuse ca fiind foarte eficient în îmbunătățirea securității cibernetice.
Un domeniu cheie diferențiator se raportează la atacurile cibernetice de către actori ai statului național:

- 54% dintre respondenți au spus că sunt foarte îngrijorați de atacurile cibernetice ale statelor naționale.
- 55% au afirmat că guvernul trebuie să facă mai mult pentru a proteja organizațiile împotriva atacurilor cibernetice ale statelor naționale.

Ce este foarte important de conștientizat este faptul că toți cei implicați (pornind de la de la utilizatori individuali, la mici organizații, mari companii sau națiuni întregi) trebuie să accepte faptul că vulnerabilitățile informatice există, iar, amenințările cibernetice pot fi abordate proactiv (figura 8).

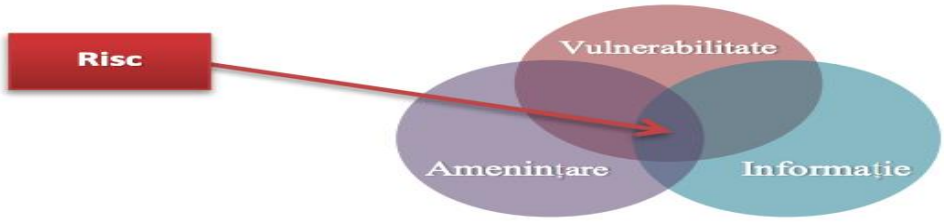


Fig. 9. Riscul de securitate cibernetică.
Sursa: https://upb.ro/wp-content/uploads/2020/03/Barbu_Ionut_Daniel_rezumat_rom.pdf.

În ceea ce privește zona de alocare de bugete și investiții putem observa din figura de mai jos că segmentul de asigurarea cibernetică la nivel global, deși a ajuns la 8 miliarde de USD, este relativ infimă dacă ne raportăm la sumele investite individual de organizații. Acest lucru confirmă încă o dată că organizațiile, indiferent de industria în care activează, preferă să își gestioneze riscurile cibernetice investind în tehnologie drept măsură defensivă.

Alternativa fiind o abordare mai generală în care se efectuează o planificare, un transfer și se implementează măsuri aferente și bune practici ce vizează o gama variantă de acțiuni cum ar fi: pregătirea adecvată a angajaților, implementarea sau actualizarea politicilor de securitate cibernetică, implementarea de proceduri si management al incidentelor, etc [31].

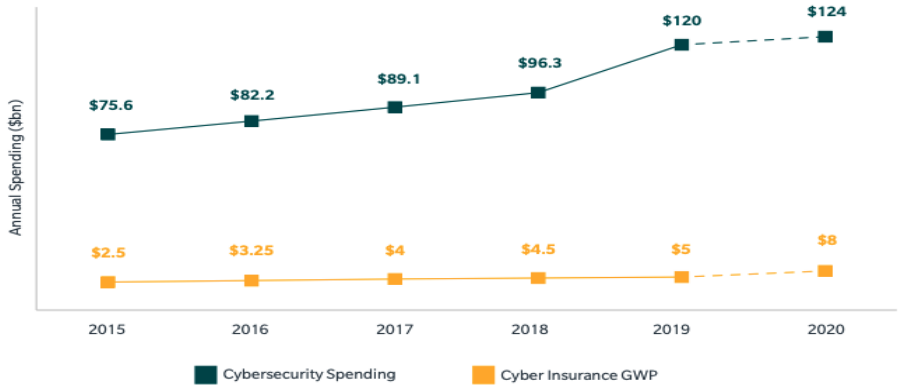


Fig. 10. Alocarea bugetelor pentru securitatea cibernetică.
Sursa: https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf.

Fiecare politică de securitate cibernetică este și poate să difere de la organizație la organizație în funcție de o multitudine de factori: domeniu de activitate, industrie, dimensiune, gradul de expunere, etc.

Cu toate acestea, drept bază, organizațiile trebuie să aibă în vedere mai multe arii cheie. Dintre ele pot fi subliniate următoarele:

- Protejarea dispozitivelor electronice personale și alte organizației:
    - Păstrarea parolelor tuturor dispozitivelor în siguranță;
    - Actualizare permanentă a software-ului antivirus;
    - Asigurarea dispozitivelor prin nesupravegherea acestora;
    - Instalare de update-uri de securitate pentru sistemul de operare, browser, etc;
    - Autentificarea pe conturile și sistemele organizației prin rețele securizate.
- Securizarea conturilor de email:
    - Evitarea deschiderii de atașamente sau link-uri externe considerat suspicioase;
    - Verificarea numelor și prenumelor celor din corespondență.
- Managementul parolelor:
    - Selectarea de parole cu minim 8 caractere (incluzând majuscule, litere mici, numere și simboluri);
    - Memorarea parolelor pentru a evita scrierea sau notarea lor. In caz contrar se recomanda utilizarea unui plugin[7] sau aplicații dedicate de la un furnizor verificat;
    - Schimbarea parolelor la fiecare doua sau trei luni.
- Transferul de date securizat:
    - Evitarea transferului sensibile de date pe alte conturi sau dispozitive, iar, atunci când este cazul să se apeleze la specialiști în securitate;
    - Transferul de date confidențiale este efectuat doar prin rețeaua securizată a organizației și nu prin rețele publice sau private Wi-Fi;
    - Obținerea de asigurări adiționale că receptorii acestor date sunt persoane autorizate și au acces de securitate adecvat;
    - Raportarea fraudelor sau potențialelor breșe de securitate.
- Măsuri adiționale:
    - Blocarea sau închiderea dispozitivelor la părăsirea birourilor;
    - Raportarea echipamentelor furate, pierdute sau deteriorate cât de curând posibil;
    - Schimbarea tuturor parolelor de acces în momentul în care un dispozitiv este furat sau pierdut;
    - Raportarea amenințărilor percepute sau posibile breșe de securitate observate;
    - A nu descărca programe software suspicioase, neautorizate sau ilegale pe echipamentele organizației;
    - Evitarea accesării website-urilor suspicioase.
- Politici pentru angajații ce lucrează în sistem WfH / Remote[8]. Se recomandă utilizarea tuturor măsurilor de encriptare și securitate luând în considerare că se utilizează rețele ce nu sunt alte organizației iar riscurile sunt crescute. Clienți de tip VPN[9] sunt recomandați și în cele mai multe cazuri sunt obligatorii în funcție de tipul de date accesate;
- Măsuri disciplinare pentru angajații sau colaboratorii ce nu respectă politicile de securitate ale organizației în funcție de gravitate (fiecare incident este analizat de la caz la caz):
    - Prima abatere, neintenționată, breșă de securitate de dimensiuni scăzute: avertisment verbal și oferirea de training pe zona de securitate;
    - Abatere repetata, intenționată, breșă de securitate de dimensiuni mari (care au cauzat pierderi financiare sau alte daune): acțiuni disciplinare severe ce pot ajunge până la concediere și / sau urmărire în instanță pentru recuperare daune după caz;
    - Adițional, angajații care sunt observați că nu respectă constant instrucțiunile de securitate urmează a fi avertizați disciplinar pentru comportamentele lor [32].

[7] Pugin – componentă de tip software ce adaugă funcționalități suplimentare unui program existent
[8] Work from home / remote – muncă în format hibrid sau de acasă
[9] VPN – Virtual Private Network

Capitolul 2. Atacuri cibernetice și cele mai uzuale breșe de securitate

Cum nivelul tehnologic s-a tot schimbat în ultimii ani, iar, progrese consistente au fost remarcate din perspectiva accesului la tehnologie, viteză de calcul și accesibilitate, era practic inevitabil ca următoarea etapă în cursa spre mai mult, spre dezvoltare, să nu mâne statele, guvernele și organizațiile într-o cursă digitală. Acest „război" digital vine din dorința de controla informația, de a putea prezice care va fi următoare mișcare a adversarului / competitorului tău, cu alte cuvinte de a avea câștig de cauză.

Această dependența a statelor a fost accentuată din ce în ce mai mult din prisma utilizării sistemelor informatice în gestionarea societății, cu toate acestea, atacuri ostile au fost înregistrate într-un număr în creștere pentru a avea acces la servere și informațiile stocate pe acestea [33].

2.1. Definire concept: atac cibernetic

Mergând mai departe în această în această analiză, avem nevoie să clarificăm ce înseamnă această sintagmă și care este motivul apariției ei. Termenul s-a popularizat gradual de-a lungul anilor și a căpătat amploare în ultima perioadă prin prisma incidentelor și breșelor apărute.

Conform NIST – Computer Security Resource Center, atac cibernetic este clasificat ca orice tip de activitate rău intenționată care încearcă să colecteze, să perturbe, să infirme, să degradeze sau să distrugă resursele sistemului informațional sau informațiile în sine.

De asemenea, un atac, prin intermediul spațiului cibernetic, care vizează utilizarea de către o organizație a spațiului cibernetic în scopul perturbării, dezactivării, distrugerii sau controlului rău intenționat a unui mediu/infrastructură de calcul; sau distrugerea integrității datelor sau sustragerea de informații controlate este catalogată ca fiind atac cibernetic [34].

Nenumărați specialiști în domeniu au generat idei și definiții pe acest concept, iar, dintre ele, cele mai cuprinzătoare ar fi cea a lui Richard Clark care postula că atacurile cibernetice sunt acțiuni întreprinse de țări să se infiltreze în calculatoarele sau rețelele de calculatoare ale unei țări sau alte țări pentru a provoca daune sau perturbări [35].

În analiza și critica acestei definiții, se poate spune că cele trei elemente, și anume autorul atacului, scopul și intenția atacului, au fost folosite drept criterii fără a lua în considerare formele de perturbare. Similar avem abordarea propusă de Michael Hayden care afirmă că atacul cibernetic este cuantificat ca fiind orice încercare intenționată de a perturba sau distruge rețelele de informatice ale unei alte țări. Evident, această definiție este, de asemenea, foarte generală și nu face distincția între criminalitatea cibernetică, atacul cibernetic și războiul cibernetic, iar linia dintre detectarea lor este într-o aură de ambiguitate [36].

Dar care este motivația și cum sunt impactate administrațiile publice și guvernamentale? Aceasta este una dintre cele mai dificile întrebări pentru că implicațiile ei merg mai departe decât pierderile materiale ale unor atacuri cibernetice clasice, putem să vorbim de pierderi de vieți omenești sau poate chiar inițierea unui noi război mondial. Câteva dintre consecințele atacurilor sunt:

- Răsturnarea sistemului de guvernare sau amenințarea catastrofală la adresa securității naționale;
- Inițierea simultană a războiului fizic sau revoltelor;
- Distrugerea catastrofală sau deteriorarea imaginii țării la nivel internațional;
- Distrugerea sau deteriorarea catastrofală a relațiilor politice și economice ale țării;
- Pierderi umane extinse sau pericol pentru sănătatea publică și siguranță;
- Haos intern;
- Perturbare administrativă la nivel național;
- Distrugerea încrederii publicului sau a credințelor religioase, naționale și etnice;
- Daune grave aduse economiei naționale;

- Distrugerea extinsă sau perturbarea performanței ale activelor cibernetice naționale [37].

Pentru a înțelege amploarea fenomenului și numărul atacurilor cibernetice ce au avut loc în ultimii ani, AAG a generat un raport statistic ce evidențiază creșterea numărului de infracțiuni cibernetice. Potrivit datelor, criminalitatea cibernetică a crescut cu 358% în anul 2020 față de anul precedent ca urmare a transferului muncii de la birou în mediul online, schimbare ce a fost impusă de pandemia de COVID-19. În următorul an, 2021, a fost înregistrată o creștere globală cu 125% a numărului de atacuri cibernetice. Aceeași statistică scoate în evidență și următoarele date:

- Aproape 1 miliard de email-uri au fost expuse atacurilor cibernetice într-un singur an, astfel fiind afectați 1 din 5 utilizatori de internet;
- În medie, scurgerile de date ale companiilor au produs daune de 4.35 milioane de dolari în anul 2022;
- În prima jumătate a anului 2022 au fost înregistrate peste 236 de milioane de atacuri cibernetice la nivel global;
- În Statele Unite 1 din 10 organizații beneficiază de o poliță de asigurare împotriva atacurilor cibernetice.

Un procent de 39% din companiile ce își desfășoară activitatea în Marea Britanie au raportat că au suferit atacuri cibernetice asupra datelor [38].

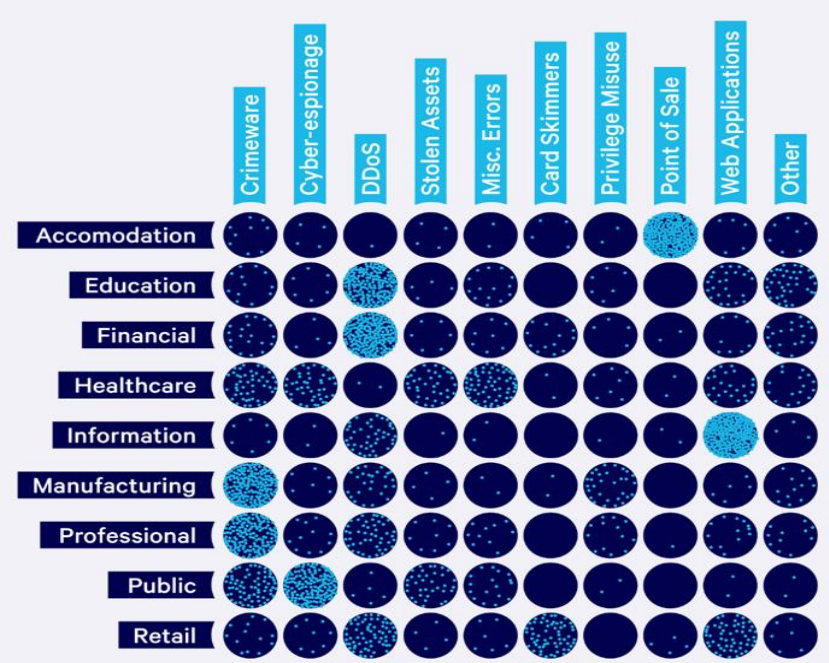


Fig. 11. Atacuri cibernetice în funcție de tip și industrie.
Sursa: https:// https://www.embroker.com/blog/cyber-attack-statistics/.

2.2. Evoluție atacuri cibernetice

Încă din cele mai vechi tipuri criminalitatea a prosperat în diferite forme, iar, zona cibernetică nu face excepție. Trebuie ținut cont de faptul că se estimează ca este o industrie de aproximativ 1.5 trilioane USD și este într-o continuă creștere [39]. De asemenea, sunt estimări că până în anul 2025 sa se atingă o cifra de 10.5 trilioane USD. [40]

Cum filozoful spaniol George Santayana a spus în lucrarea sa „cei ce nu își cunosc trecutul sunt condamnați în a-l repeta" este necesar să înțelegem care au fost principalele momente în dezvoltarea acestui concept pentru a putea face pasul următor în cunoștință de cauză [41].

Analizând informațiile disponibile putem observa că printre primele atacuri cibernetice ce a avut loc și a fost consemnat s-a petrecut în Franța anului 1834 când telegraful era în apogeu tehnologic.

Frații Blanc erau implicați în tranzacționarea cu obligațiuni guvernamentale la bursa din Bordeaux. Similar cu ce se întâmplă și în prezent, cel ce deține informația într-un timp mai scurt, are câștig de cauza, iar, în vremea respectivă putea dura până la câteva zile ca informații de la Paris sa ajungă.

Așadar atacatori au reușit să obțină accesul la sistemul național telegrafic mituind un operator și au furat informații cu privire la evoluția pieței financiare. Înșelătoria a fost depistată în anul 1836 când operatorul implicat s-a îmbolnăvit și a simțit nevoia să spună ce a făcut. Deși frații Blanc au fost aduși în fața justiției pentru faptele sale, aceștia nu au fost condamnați întrucât nu existau reglementări sau legi sa acopere speța în cauză [42].

În 1940, Rene Carmille a devenit primul hacker etic. A fost expert în calculatoare cu cartele perforate (punch cards) și membru al Rezistenței din Franța în timpul ocupației naziste. El deținea mașinile pe care guvernul francez le folosea pentru a procesa informații, a descoperit că naziștii foloseau mașinile pentru a-i urmări pe evrei, așa că s-a oferit să le permită să-și folosească mașina. Au luat momeala, iar apoi a folosit accesul primit pentru a-i sparge și a le perturba eforturile.

În 1962, primele parole pentru computer au fost create de MIT pentru a limita timpul petrecut de studenți pe computer și pentru a oferi confidențialitate utilizatorilor. Allan Scherr, un student la MIT, a creat un card perforat care a declanșat computerul să imprime toate parolele din sistem. Apoi le-a folosit pentru a obține mai mult timp pe calculator și le-a distribuit și prietenilor săi, de asemenea, au piratat conturile profesorilor, și le-au lăsat mesaje batjocoritoare, acesta a recunoscut evenimentul 25 de ani mai târziu.

Se crede că primul virus informatic a fost folosit în 1969 la centrul de calculatoare al Universității din Washington, o persoană care nu a fost numită niciodată a instalat pe unul dintre computere un program care a ajuns să fie cunoscut sub numele de „Virus RABBITS”. Programul a început să se repete până când a copleșit computerul, făcându-l să se închidă.

Kevin Mitnick este adesea menționat drept primul criminal cibernetic, din 1970 până în 1995, Mitnick a reușit să acceseze unele dintre cele mai păzite și mai sigure rețele din lume, inclusiv Motorola și Nokia. El a folosit scheme complexe de inginerie socială care au păcălit personalul cheie din companii pentru a-i oferi parole și coduri pe care le-a folosit pentru a pătrunde în sistemele informatice interne. El a fost arestat de FBI și s-a confruntat cu o serie de acuzații federale. După închisoare, Mitnick a devenit consultant și autor de securitate cibernetică.

În anul 1971 istoria securității cibernetice începe cu adevărat prin Bob Thomas, un programator de computer pentru BBN, a creat și a implementat un virus care a servit drept test de securitate. Nu a fost rău intenționat, dar a evidențiat zone de vulnerabilitate și defecte de securitate în ceea ce avea să devină „internetul”.

Virusul, numit după un răufăcător al lui Scooby Doo, „Creeper”, a fost conceput pentru a se muta pe ARPANET[10] – precursorul a ceea ce numim acum internet ARPANET a fost înființat de DoD[11].

Thomas a creat virusul pentru a fi un program experimental nedăunător, auto-replicabil. A fost menit să ilustreze modul în care funcționează aplicațiile mobile, dar, în schimb, a corupt calculatoarele de tip mainframe DEC PDP-10[12] de la Digital Equipment Corporation, interferând cu ecranele computerelor de teletype care erau conectate. Tot ceea ce utilizatorii puteau vedea pe ecran erau cuvintele „Eu sunt târâtoarea, prinde-mă dacă poți!”.

[10] ARPAN - Advanced Research Projects Agency Network

[11] DoD – Department of Defence – În traducere din limba engleză Departamentul de Apărare al Statelor Unite

[12] DEC PDP-10 – Calculator de tip mainframe fabricat în ani 1960 - 1983

Ca răspuns, Ray Tomlinson, colegul lui Thomas, a creat Programul Reaper. Era asemănător cu Creeper-ul. Se deplasează prin internet, replicându-se și găsește copii ale Creeper. Când localizează copiile, le deconectează, astfel încât acestea devin impotente. Reaper a fost prima încercare de securitate cibernetică – primul program software antivirus [43].

În anul 1981, după ce a pătruns cu succes în sistemele interne ale AT&T[13] și a schimbat ceasurile computerelor lor, făcând ravagii, Ian Murphy a devenit prima persoană care a fost găsită vreodată vinovată de comiterea unei infracțiuni cibernetice.

Primul atac cibernetic important ce a avut loc pe internet a venit prin intermediul lui Robert Morris în anul 1988, la momentul respectiv student în cadrul Universității Cornell din New York. „Morris Worm" a proiectat un nou tip de virus care a infectat sisteme informatice de la Stanford, Princeton, Johns Hopkins, NASA[14], Lawrence Livermore Labs și UC Berkeley, printre alte instituții. Noutatea pe care a adus-o a venit din faptul că acesta se putea răspândi fără ajutorul unui program gazda.

Deși Moris Worm s-a limitat la computerele cu anumită versiune de Unix și nu corupt sau stres fișiere, acesta încetinit considerabil activitatea în diferite organizații private sau guvernamentale. Din estimările efectuate la acea vreme daunele cauzate variază între 100.000 și câteva milioane de USD. FBI[15] a intervenit și a lansat o anchetă ce s-a finalizat prin audierea și condamnarea lui Robert Morris la 400 de ore de muncă în folosul comunității și o amendă [44].

În anul 1994, împreună cu răspândirea la scară largă a internetului avem consemnat următorul eveniment notabil în istori și anumite cazul lui Richard Pryce și Matt Bevan sub pseudonimele lor Datastream Cowboy și Kuji. Aceștia au folosit un program de „sniffer" pentru a lansa o serie de atacuri și au accesat sistemele Pentagonului.

Un an mai târziu, un grup de hackeri ruși sunt arestați la Londra după ce au spart sistemele informatice de la Citibank și au furat peste 10 milioane de dolari, unul dintre puținele cazuri de fraudă informatică care au ajuns în ziare. Trei dintre complicii implicați au fost arestați în Israel, Olanda sau Statele Unite.

Ulterior, Vladimir Levin a fost si el arestat în Londra și extrădat pentru a fi judecat si condamnat. Camera Internațională de Comerț a recunoscut recent că a avut cunoștință de o serie de cazuri de accesare neautorizata cibernetică și furt, însă, cu toate acestea, deloc surprinzător, nicio altă instituție financiară britanică nu a recunoscut vreodată că a fost vizată de hackeri [39].

Max Butler, un consultant de securitate pentru FBI, printre altele, a spart site-urile web ale guvernului SUA sub pretexte false. U.S. Air Force a alertat oficialii cu privire la faptele sale, iar el a primit o condamnare de 18 luni. Ulterior, pentru o altă incursiune ilicită, a fost condamnat la 13 ani, record pentru un hacker.

Virușii informatici au fost relativ necunoscuți de publicul larg până când Virusul Melissa a lovit în martie 1999 și a afectat utilizatorii de pe internet, corupându-le fișierele documentelor Microsoft și cauzând daune estimate la 80 de milioane de dolari. Acesta a fost dezvoltat de către David Lee Smith și a fost răspândit prin postarea pe un grup de știri un fișier cu denumirea „alt.sex" [39].

---

[13] AT&T – una dintre cele mai mari și importante companii de telecomunicații din Statele Unite ale Americii

[14] NASA – National Aeronautics and Space Administraton – În traducere din limba engleză Administrația Națională Aero Spațială

[15] FBI – Federal Bireau of Investigation – În traducere din limba engleză Biroul Federal de Investigații

Anii 2000 au început cu o mulțime de noutăți din perspectiva complexității metodelor utilizate de atacatori, iar, în egală măsură și identificarea de soluții pentru prevenirea lor pe viitor.

Un hacker în vârstă de 15 ani pe nume Michael Calse – care utiliza pseudonimul „Mafiaboy" – a lansat o serie de atacuri DDoS[16] asupra unora dintre cele mai mari site-uri comerciale din lume, site-uri precum Amazon, Yahoo, CNN și eBay. Atacul a dus la blocarea site-urilor ore în șir în unele cazuri și a costat aceste afaceri milioane de nespus.

În 2005 o încălcare a securității la un comerciant, deși nu a fost recunoscut oficial niciodată se consideră că era vorba despre Polo Ralph Lauren, a dus la o scurgerea de date a 1.4 milioane de utilizatori HSBC Bank având carduri MasterCard.

În 2008, într-una dintre cele mai mari breșe de până acum ca valoare, sistemele Heartland Payment au fost atacate folosind o combinație de SQL injection, sniffer de parole și programe malware[17], compromițând datele a 134 de milioane de utilizatori. Acest atac a generat pierderi de peste 200 milioane de USD. Ca urmare, în 2009 Albert Gonzalez a fost arestat împreună cu doi complici pentru faptele săvârșite și condamnat la 20 de ani de închisoare.

Începând cu anii 2010, zona de criminalitate cibernetică a căpătat amploare făcând primii pași serioși în a ajunge la cifrele impresionante menționate în la începutul capitolului.

Viermele Stuxnet – numit prima „armă digitală" din lume – a atacat centralele nucleare din Iran, sabotând instalațiile de îmbogățire a uraniului din țară, iar, ulterior s-a răspândit și la alte facilități industriale și producătoare de energie. Virusul era capabil să atace componente hardware ale sistemelor infectate, în special PLC-uri[18] Acest vierme a fost conceput de de NSA[19], CIA[20] si Mossad[21].

Virusul troian Zeus a fost distribuit în întreaga lume prin e-mail într-un atac care a vizat organizațiile de servicii financiare. Acesta utiliza în principal keylogger-ul browser-ului pentru a obține acces șa informațiile bancare ale unui computer infectat. Este aproape imposibil de menționat cine este în spatele virusului, cu atât mai mult cu cât codul a luat amploare și au apărut o multitudine de versiuni, unele ce rulează chiar și în prezent.

Într-un atac notoriu, Operațiunea Aurora a fost lansată de hackeri militari chinezi asupra a peste 20 de companii de tehnologie de top **(**Adobe, Juniper Networks, Rackspace, Yahoo, Morgan Stanley, etc). Publicul a fost informat pentru prima dată despre atacuri atunci când Google a notificat publicul că proprietatea sa intelectuală a fost confiscată în urma atacului.

Sony Corporation a anunțat în aprilie 2011 că, în decurs de câteva zile, hackerii au furat informații de la 77 de milioane de utilizatori ai PlayStation Network, acestea includeau numele de utilizator și parolele jucătorilor, datele lor de naștere, răspunsuri la întrebările de securitate și multe altele. Pentru a remedia această problemă experții în securitate cibernetică de la Sony au avut nevoie de 23 de zile pentru a recupera accesul la sistem și a remedia problema.

Doi ani mai târziu, în probabil cea mai mare scurgere de date de profil înalt din toate timpurile, denunțătorul Edward Snowden a dezvăluit informații sensibile furate de la mai multe guverne străine cu software spyware, ca parte a programului de supraveghere PRISM al NSA.

---

[16] DDoS – Distributed Denial of Service – tip de atac cibernetic prin care atacatorul inundă un server cu informații pentru a bloca accesul utilizatorilor la un anumit site sau serviciu
[17] Malware – program software instalat pe calculatorul unui utilizator fără consimțământul acestuia
[18] PLC – Programmable Logic Controller – În traducere din limba engleză controlor logic programabil
[19] NSA – National Security Agency – În traducere din limba engleză Agenția Națională de Securitate
[20] CIA – Central Intelligence Agency – În traducere din limba engleză Agenția de Centrală de Informații
[21] Mossad – Institutul National de Inteligență și Operațiuni Speciale ale Israelului

Tot în 2013 ani mai târziu, un alt gigantic american din industria comerțului, Target, a fost vizat de un atac de tip phishing. În acest fel, datele bancare a peste 110 milioane de clienți Target au fost furate prin intermediul unui email ce conținea un malware. Începând cu 2015 au apărut primele tulpini ale ransomwar-ului SamSam, care până în 2018 i-a adus creatorilor săi, Mohammad Mehdi Shah Mansouri și Faramarz Shahi Savandi, aproape 6 milioane de dolari. Printre cele mai importante atacuri de „luare de ostatici" au fost orașul Atlanta și Departamentul de Transport din Colorado.

Un atac de tip spear-phishing de succes împotriva țintelor de mare valoare ale DoD cu e-mailuri personalizate a dus la o încălcare a informațiilor pentru 4.000 de militari și civili care lucrau pentru șefii de stat major comun. Atacul a forțat Pentagonul să-și închidă sistemul de e-mail. În 2016 firma aerospațială austriacă, FACC AG[22], a fost fraudată cu 50 de milioane de euro într-o schemă de spear-phishing care a păcălit un angajat din departamentul financiar să transfere fondurile în conturi bancare controlate de infractorii cibernetici. Ca urmare, CEO-ul companiei a fost concediat.

Poate cea mai insidioasă dintre toate tulpinile de ransomware, WannaCry, a reușit să afecteze peste 200.000 de computere Windows din 150 de țări. A fost deosebit de periculos - și mortal - deoarece spitalele Serviciului Național de Sănătate din Marea Britanie au fost printre cele mai devastate. Se presupune pe scară largă că hackerii din Coreea de Nord s-au aflat în spatele atacului. Doar o lună mai târziu, utilizând succesul WannaCry a apărut NotPetya, o versiune actualizată a tulpinii anterioare de ransomware. A luat organizații de la gigantul de transport maritim Maersk la producătorul multinațional de produse farmaceutice Merck.

În cea mai mare inundație DDoS de până acum (2018), GitHub – o platformă populară pentru dezvoltatori – a înregistrat un trafic de 1,3 terabytes pe secundă, ceea ce a oprit toate operațiunile pe serverul său. GitHub avea măsuri de securitate în vigoare, mult mai mult decât majoritatea organizațiilor, dar a fost pur și simplu copleșit de dimensiunea mare a atacului.

De asemenea, poate că cel mai demn de remarcat dintre toate atacurile de criptojacking a fost Coinhive, un serviciu popular de exploatare a criptomonedei care, pentru o vreme, a fost considerat de către firmele de securitate de top drept principala amenințare rău intenționată pentru utilizatorii web. Codul său de computer ar putea fi folosit pe site-uri web piratate pentru a fura puterea de procesare a dispozitivelor vizitatorilor site-ului respectiv. Timp de 15 luni lungi, infractorii cibernetici au folosit programul rău intenționat pentru a infecta milioane de dispozitive.

2019 a marcat incidentul cu Capital One, victima uneia dintre cele mai mari breșe de date din istoria bancară, când au fost accesate peste 100 de milioane de aplicații pentru carduri de credit și au fost preluate mii de numere de securitate socială și de cont bancar. Capital One a cheltuit aproximativ 150 de milioane de dolari pentru atenuarea daunelor.

În anul 2020, atacurile cibernetice rusești asupra instituțiilor guvernamentale americane au fost în creștere și, într-una dintre cele mai catastrofale breșe de date, agenții de informații străini au profitat de un program compromis SolarWinds și au invadat aproximativ 18.000 de rețele private și afiliate guvernului. Aceste încălcări de date au permis atacatorilor acces la o abundență de informații identificabile, inclusiv informații financiare, cod sursă, parole și nume de utilizator.

În 2022 un hack de la mijlocul lunii septembrie, a scos o cantitate uimitoare de material de la un titan al industriei jocurilor de noroc, lansarea foarte anticipată a lui Rockstar Games Grand Theft Auto 6, a fost aruncată în haos când un hacker cunoscut sub numele de „teapotuberhacker" a spart canalul intern de Slack al Rockstar, și a furat 90 de videoclipuri cu un joc în curs de desfășurare.

[22] FACC - Fischer Advanced Composite Components. Companie de top Austriacă ce activează în industria aeronautică

Dar acest hacker nu a terminat, într-un atac Slack extrem de similar, teapotuberhacker și-a respectat pseudonimul, iar pe 14 septembrie când a spart Uber. Compania internațională de ridesharing a fost agresată, hackerul obținând „acces aproape complet la Uber”, inclusiv sisteme de e-mail, comunicații interne, stocare în cloud și depozite de coduri [30].

Deși am adus în discuție un număr restrâns de exemple din limită de spațiu, am preferat să ne concentrăm pe unele dintre cele mai reprezentative incidente cibernetice pentru a avea ceva mai multe informații despre care a fost evoluția fenomenului în lume.

Continuăm să explicăm cum funcționează spionajul cibernetic, vom pătrunde într-o misiune din viața reală, care a avut loc în îndepărtatul Orient Mijlociu, s-a înțeles cel mai probabil deja intenția, că facem referire la infiltrarea într-o instalație nucleară pentru a proteja lumea de posibile amenințări militare nucleare.

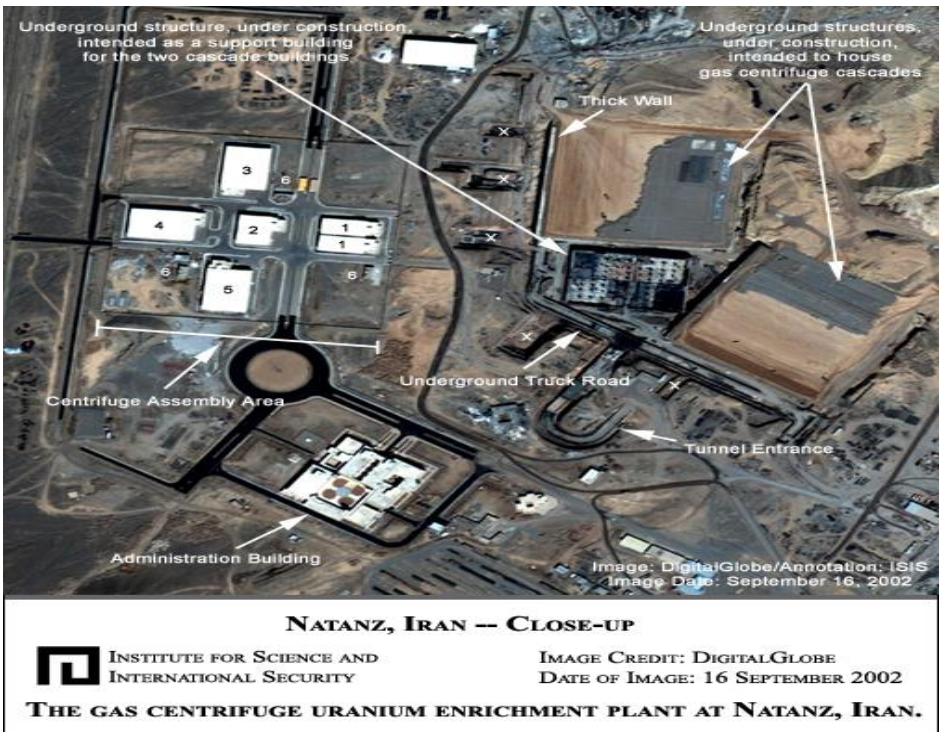


Fig. 12. Uzina iraniană de îmbogățire a uraniului cu centrifugă cu gaz de la Natanz.
Sursa: https://isis-online.org/publications/iran/natanz03_02.html.

Aliații au avut dreptate să își facă griji că Iranul folosea instalațiile de centrifugare ale bazei, pentru a crea mai mult combustibil decât era necesar pentru a genera electricitate, și utlizau centrifugele pentru a crea combustibil nuclear pentru arme atomice.

Aceste centrifuge trebuie să fie distruse, dar ce să facă au fost luate în considerare mai multe opțiuni, dar nu au putut fi trimiși soldați, baza este în mijlocul țării, este imposibil să nu fie detectați, au vrut să trimită avioane de luptă care să bombardeze și să arunce totul în aer, însă o astfel de operațiune ar fi una riscantă și murdară, ceea ce nu ar fi un exercițiu de PR bun (C. Vrabie, 2023).

Așa că în loc să lanseze bombe sau să trimită agenți, aceștia au ales să lanseze un vierme informatic, iar operațiune care a devenit cunoscută sub numele de Jocurile Olimpice (Operation Olympic Games), tot ce trebuie să facă era să plaseze într-un fel sau altul vieremele în interior. Există multe moduri în care pot face acest lucru, dar din păcate, nu putem intra în detalii aici. Cu toate acestea, există o metodă care este cea mai cunoscută, și pe care o vom expune în continuare [46].

În primul rând virușii informatici au fost introduși în stick-urile de memorie USB, au fost apoi plasați în jurul bazei, profitând de orașele învecinate - inclusiv Teheran, unde unii ofițeri se presupune că își petrec viața. Unii dintre aceștia au reușit să pună mâna pe aceste stick-uri, și să le conecteze la computere personale – laptopuri sau PC-uri (C. Vrabie 2023). Această abordare este necesară deoarece baza nucleară Natanz nu era conectată la internet [46].

În acest mod au pătruns agenţii electronici şi au făcut ceea ce trebuie să facă toți agenții buni, au început lucrările de recunoaștere, au început să intre în rețea, „mergând pe coridoare" căutându-și țintele. Țintele sunt cutiile SIEMENS care conțin controlere pentru centrifuge, iar odată descoperite, un rootkit a fost lansat împreună cu întregul arsenal de arme necesare unui atac digital care urma să se petreacă (C. Vrabie 2023). În acest fel parametrii de funcționare ai controlerelor, și într-adevăr parametrii de funcționare ai aplicațiilor pe care le gestionează au fost alterați.

Ulterior agentul a „telefonat" acasă în diferite moduri, și au predat comanda controlelor Statelor Unite și Israelului, care au ordonat centrifugelor să se învârtească la un asemenea nivel încât să nu mai funcționeze luni de zile, fără ca agenți umani să pună piciorul facilități iraniene. Programul a fost un success, a încetinit programul de dezvoltare nucleară al Iranului, iar în acest mod planurile nucleare ale Iranului au fost trimise înapoi cu câțiva ani.

Cu toate acestea apare o problem, aliații care au petrecut atât de mult timp obținând acest agent electronic, încât nici nu s-au gândit la ce s-ar întâmpla dacă ar acesta ar ieși afară ulterior acesta asta a și făcut, aplicația și-a făcut treaba în continuare. A început să caute alte ținte, alte controloare Siemens, mai întâi în Iran și în Orientul Mijlociu, apoi în Europa, ulterior de acolo a plecat în alte părți ale lumii, în căutarea unor instalații nucleare, trebuie menționat faptul că acest spion își cunoaște foarte bine sarcina (C.Vrabie 2023).

Acesta căuta anumiți controloare – cele cu semnătura unică ca acelor din Natanz, în orice caz apărarea lui a fost spulberată, industria de securitate, mai concret Kaspersky Lab la descoperit, ceea ce a reprezentat operațiunea de preluare a controlului pentru a a proteja planeta de amenințările nucleare, devine acum Stuxnet - cea mai avansată amenințare software de până acum [46].

2.3. Descriere tipuri de atacuri cibernetice

Spațiul cibernetic este un mediu ce are în compoziție mai multe componente, printre care: hardware, software, internet, servicii de informare și sisteme de control. Această infrastructură este esențială pentru activitatea oricărei organizații, indiferent daca vorbim de o companie sau de un stat.

Din perspectiva amenințărilor cibernetice acestea pot clasifica în două zone principale: amenințări ce vizează informațiile și comunicările și amenințări ce se concentrează pe infrastructura tehnică.

Din prima categorie principalele amenințări sunt:
- Furtul/ publicarea informațiilor personale;
- Furtul/ publicarea informațiilor clasificate sau secrete;
- Furtul de identitate (este vorba de identitatea digitală a indivizilor);
- Frauda cibernetică;
- Spionajul industrial sau de stat.

Din categoria a doua sunt:
- Atacurile asupra sistemelor Hardware/Software;
- Atacurile asupra serviciilor de internet;
- Atacurile asupra rețelelor sau a sistemelor prin implicarea unor terți;
- Atacurile ce utilizează viermi sau viruși informatici;

O altă clasificare ce poate fi făcută este în funcție de proveniență și a impactului pe care îl au:

- Atacuri sponsorizate de state;
- Hackeri;
- Structuri organizate de hackeri;
- Teroriști;
- Personal nemulțumit din interior;
- Grupuri de sabotaj.

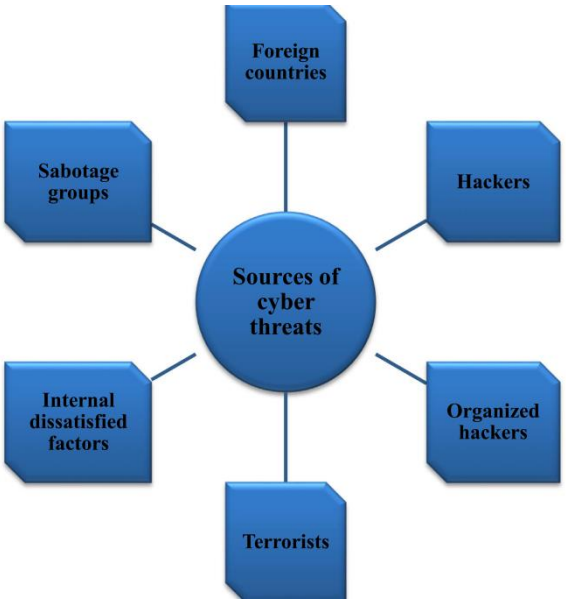


Fig. 13. Surse ale atacurilor cibernetice.
Sursa: https://www.sciencedirect.com/science/article/pii/S2352484721007289?ref=pdf_download&fr=RR-2&rr=83f34ba43c10052d.

Atacuri sponsorizate de către stat: Multe organizații private încearcă să obțină informații economice și industriale de la alte organizații concurente, acest tip de atac este adesea efectuat cu ajutorul guvernului.

Hackerii: Odată cu apariția internetului, dar mai ales în ultimii ani, activitatea hackerilor a devenit unul dintre cele mai mari pericole pentru guverne și organizații. Principiile acestei agresiuni sunt anonimatul, și transmiterea gratuită de informații prin spațiul cibernetic, în special cu ajutorul internetui. Misiunea lor este de a „ataca" spațiul cibernetic al persoanelor, companiilor, proiectelor sau alte organizații care încalcă interesele sau principiile lor.

Acest lucru înseamnă că hackerii pot hack-ui spațiul cibernetic al guvernelor din majoritatea țărilor din lume, al băncilor, al companiilor de telecomunicații, al furnizorilor de infrastructură critică, al furnizorilor de servicii de internet și, în cele din urmă, al întregului spațiu cibernetic. Obiectivul principal al acestor hack-uri este furtul de date sensibile.

Structuri organizate de hackeri: Bandele informatice, sau bandele de crimă organizată, au început să își desfășoare activitatea pe internet, profitând de anonimat. Obiectivul acestor bande este de an obține informații sensibile pentru a le folosi pentru fraudă și a câștiga bani.

Teroriști: Grupurile extremiste și terorismul folosesc spațiul cibernetic pentru a planifica și publica acțiunile lor, și pentru a racola adepți pentru a le efectua. Aceste grupuri sunt conștiente de importanța strategică și tactică an internetului pentru interesele lor, iar forumurile și rețelele sociale au devenit principalul instrument folosit.

Personal nemulțumit din interior: Aceste grupuri reprezintă una dintre cele mai mari amenințări la adresa securității spațiului cibernetic al națiunilor, companiilor și proiectelor, deoarece acestea sunt de multe ori componente esențiale ale tuturor atacurilor menționate mai sus. Aceste atacuri pot include spioni infiltrați de stat, angajați nemulțumiți, bande de teroriști sau infractori cibernetici.

Grupuri de sabotaj: Aceste grupuri țintesc scoaterea din funcțiune temporară sau poate chiar distrugerea în întregime a obiectivelor avute în vedere [37].

Spațiul virtual sau cibernetic este structurat pe trei straturi suprapuse: un strat fizic, un strat logic și un strat social, care sunt, la rândul lor, formate din cinci componente: componenta geografică, componenta fizică de rețea, componenta logică de rețea, oameni și identități cibernetice.

- Nivelul fizic:
  - componenta geografică;
  - componenta fizică de rețea;
- Nivelul logic:
  - componenta logică de rețea;
- Nivelul social:
  - Interfețe;
  - identități cibernetice.

Stratul fizic cuprinde componenta geografică şi componenta fizică a rețelelor. Componenta geografică se referă la locația fizică a elementelor de bază ale componentelor fizice ale rețelelor. Componenta fizică de rețea este alcătuită din hardware și infrastructuri care să sprijin erețelele și conectoriilor fizici (cabluri, routere, servere, calculatoare etc.).

Nivelul logic este format din componenta logică a rețelelor, acestea sunt conexiuni logice care există între nodurile rețelelor, un nod putând fi orice dispozitiv careeste conectat la rețeaua de comunicații și sisteme IT.

Stratul social este alcătuit din oameni și identități cibernetice. Componenta „oameni” este formată din persoanele care interacționeaza în spațiul cibernetic. Aceste identități cibernetice pot fi reale sau false, care permite utilizatorului să se bucure de anonimat și face dificilă urmărirea comportamentului infracțional care are loc în spațiul cibernetic. Identitățile cibernetice sunt formate din, printre altele, conturi de email, conturi de utilizator de rețea și profilurile de social media etc. [45]

Mergând mai departe în încercarea noastră de a structura această zonă complexă, suntem obligați sa ne concentram pe posibilele tipurile de atacuri cibernetice.

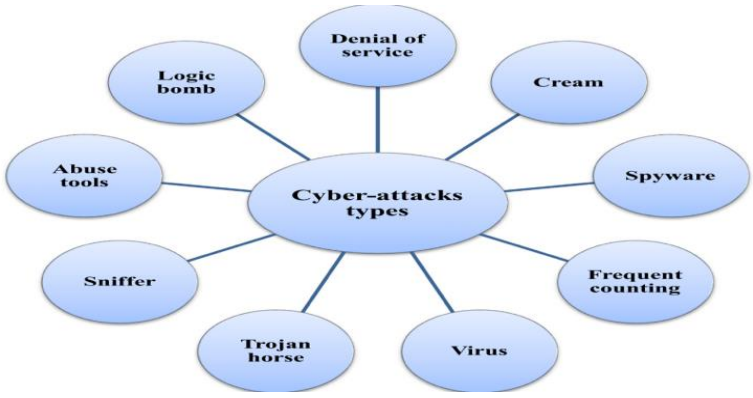


Fig. 14. Principalele tipuri de atacuri cibernetice.
Sursa: https://www.sciencedirect.com/science/article/pii/S2352484721007289?ref=pdf_download&fr=RR-2&rr=83f34ba43c10052d.

Denial of Service: atacurile DoS vizează să facă indisponibil un serviciu, site web sau rețea prin inundarea cu trafic artificial. În cazul atacurilor DDoS, traficul provine de la multiple surse.

Spyware: urmăresc acțiunile victimei atât local cât și ca activitatea pe internet. Pot colecta parole, informații bancare, email-uri și pot să includă inclusiv urmărirea tastelor apăsate

Viruși: aceștia se răspândesc de la calculator, la calculator fie prin descărcare de fișiere sau programe. Pentru infectare este necesară acțiunea utilizatorului

Troienii: de regula este ascuns în diferite programe care nu par a fi dăunătoare. După instalare deschide căi de acces pentru hackeri pentru a pătrunde în sistem.

Sniffer: De asemenea, un program care se uite după anumite tipuri de informații (ex. parole) examinând fiecare pachet din fluxul de date

Abuse tools: Sunt disponibile publicului pentru detecția și introducerea de vulnerabilități în rețele cu diferite niveluri de calificare

Bombe logice: Un alt tip de atac în care un programator introduce codul într-un program în care, în cazul unui anumit eveniment, programul realizează automat o activitate distructivă

Principalii vectori de infectie folositi de un atac ransomware sunt:
- mailuri de tip phishing;
- site-uri web compromise;
- protocolul RDP[23];
- exploit kit-uri;
- reclame malitioase (malvertising);
- download-uri;
- aplicatii de messaging;

Phishing-ul înca se păstrează drept cea mai comună metodă folosită de atacatori pentru a infecta un dispozitiv cu ransomware. Victimele sunt păcălite să dea click pe un link inclus în mesaj sau să descarce un fi șier malițios atașat prin email- uri foarte bine create , cu informații personalizate și specifice menite să câștige încrederea victimei. Fișierele malițioase pot arată la fel că fișierele normale, și atacatorii pot profită de faptul că Windows-ul ascunde în mod implicit extensia unui fișier .

De exemplu, un fișier anexat se poate numi “document.pdf”, însă numele real poate fi “document.pdf.exe” după examinarea extensiei. Cele mai folosite tipuri de fișiere pentru a răspândi ransomware, dar și alte forme de malware, sunt documentele Office, fișierele pdf și arhivele. GandCrab, Cerber, CryptoWall și Locky sunt variante de ransomware care folosesc phishing-ul că metodă de infecție .

Site-urile web compromise sunt o altă metodă preferată de hackeri pentru a răspândi ransomware. Atacatorii reușesc să profite de anumite vulnerabilități ale serverelor web și să injecteze cod malițios în paginile web ale site -ului. Atunci când victima vizitează site-ul, care de altfel poate fi complet legitim, acesteia i se poate cere să descarce o versiune nouă a unui software, de exemplu de browser web sau de plugin. Dacă utilizatorul da click, ransomware-ul se poate activă direct sau se rulează un script care descarcă și activează ransomware-ul. Exemple de ransomware care folosesc site- uri compromise că mecanism de propagare sunt GandCrab, Cerber și Revil.

RDP permite administratorilor IT să acceseze și să controleze un calculator de la distanță , însă acest lucru ar trebui făcut printr-o rețea securizată și nu direct prin Internet. Atacatorii pot folosi

[23] RDP – Remote Destop Protocol.

unelte precum Shodan sau Nmap pentru a identifica mașini expuse în Internet care au portul deschis de RDP.

O dată identificate aceste mașini , atacatorii pot folosi unelte open source precum “John the Ripper” sau “ Cain and Abel” pentru a execută atacuri de tip “brute force” pentru a ghici parolă de acces. După ce atacatorii au acces pe sistem , își pot escalada privilegiile și pot descarcă și execută ransomware, pot pivotă și spre alte sisteme pentru a mari gradul de infecție . SamSam este un tip de ransomware care exploatează RDP-ul pentru a compromite sisteme slab protejate care folosesc acest serviciu.

Exploit kit-urile sunt programe software micuțe care sunt construite cu scopul de a exploata o vulnerabilitate cunoscută a unui sistem de operare sau aplicație , că de exemplu Java sau Adobe Flash. GandCrab, Cerber Locky și CryptoWall sunt variante de ransomware livrate prin acest vector folosit în site - uri compromise sau prin campanii de malvertising.

Malvertising-ul se poate folosi de anumite vulnerabilități din browser-ul web care nu a fost patch-uit la timp pentru a afișa reclame online care conțin cod malițios . La execuția acestui cod se va descarcă ransomware care va începe infecția stației compromise. Deși este un mijloc de propagare mai puțin utilizat, malvertising-ul este periculos întrucât nu necesită nicio acțiune explicită din partea utilizatorului.

Download-urile de fișiere , mai ales din surse dubioase sau neautorizate (site - uri de file sharing, rețele de torrente), sunt adesea folosite de hackeri pentru a- și răspândi malware-ul. Alte surse similare de ransomware sunt software-uri integrate în alte programe care fac “piggybacking” și se instalează o dată cu programul principal, programe de tip crack și keygen-uri.

Aplicațiile de mesagerie instanța că Facebook Messenger sau WhatsApp pot fi folosite pentru a transmite imagini de tipul SVG sau jpeg care conțin ransomware. Imaginile SVG, de exemplu, sunt bazate pe XML, un mod de formatare a datelor care permite atacatorilor să insereze orice cod doresc, inclusiv malware. O dată accesată imaginea, această direcționează victima către un site aparent legitim de unde se descarcă ransomware-ul. [37]

Capitolul 3. Studiu de caz – Paralela între cele mai marcante incidente la nivel global

Având în vedere cele menționate anterior și faptul că ne-am concentrat pe tot ceea ce însemnă latura teoretică a conceptelor este inevitabil să nu mutăm analiza și către latura practică. Deși abordarea cea mai uzitată și simplă ar fi fost să utilizăm un exemplu pe care-l detaliem, atât din punctul de vedere al modului de acțiune al atacatorilor, cât și al daunelor provocate, s-a dorit o abordare la nivel macro.

Mai concret, în capitolul ce urmează se intenționează a creiona o „hartă" a celor mai marcante atacuri cibernetice la nivel global, având ca focus diferențele de abordare între cei mai importanți actori la nivel politico-economic (Europa, Statele Unite ale Americii, China, Rusia, etc), și care a fost abordarea utilizată în a combate aceste fenomene.

Trecând prin multiple situații de criză în ultimii ani suntem complet conștienți de faptul că latura cibernetică este cheia ce poate determina câștigarea unui conflict armat sau nu, dezvoltarea exponențială a unei organizații private, dărâmarea unui guvern sau poate chiar prăbușirea unei întregi țări. Din această perspectivă, deși nu sunt tot timpul aliniate așteptărilor companiilor din mediu privat cu modul în care guvernele legiferează, devine din ce în ce mai evident ca acest parteneriat poate să fie cheia în contextul general al acestei lucrări. Această afirmație vine în contextul în care este inevitabil ca atunci când facem referire la atacuri cibernetice sau la securitate cibernetică la nivel ce concept, inevitabil putem identifica strânse legături.

Sunt postulate mai multe teorii care subliniază această cauzalitate între toți acești factori, iar, luând în considerare conflictul armat și invazia rusă din Ucraina de la începutul lui 2022, este evident că zona de securitate informatică a fost importantă. Cu trei zile după lansarea invaziei teritoriale, oficialii europeni s-au reunit într-o ședință extraordinară cu obiectivul cum pot guvernele statelor membre să colaboreze pentru a fi capabile să respingă potențiale atacuri cibernetice asupra rețelelor esențiale.

Surprinzător a fost cu adevărat modul în care aceste atacuri care nu au întârziat să apară au eșuat. În acest caz trebuie menționat faptul că principala țintă a Rusiei a fost și este Ucraina și infrastructura ei, care deși a fost ținta atacurilor cu rachete, a continuat să funcționeze. Sistemul bancar este online, infrastructura de transport este operațională și exemplele pot să continue [38].

Ce doresc să subliniez este faptul că acest succes a fost datorat parterneriatului public-privat puternic și dorința acestora de a se concentra pe ce este important și la a renunța la idei contraproductive despre suveranitatea digitală.

Vorbind despre suveranitatea digitală ne raportăm la servicii de tip cloud[24].

În prezent oficialii ENISA[25] finalizează o schemă europeană de certificare pentru companiile de cloud pentru a dovedi că respectă standarde înalte de securitate cibernetică. Proiectul de cerințe ar putea forța giganții cloud americani să dezavueze legile Washingtonului privind accesul la date. Doar companiile europene se pot califica pentru cea mai înaltă certificare, cu excepția liderilor mondiali Amazon, Microsoft și Google [39].

Dacă va fi adoptată, acest impuls pentru dezvoltarea unei industrie cloud europene promite să fie contraproductiv. Ar forța companiile europene să folosească furnizori locali cu prețuri ridicate și cu performanțe scăzute. S-ar dovedi, în mod pervers, un risc de securitate. Experții în securitate cibernetică sunt de acord că cea mai bună modalitate de a proteja datele este de a distribui, nu de a localiza datele și de a le stoca cu cei mai mari și mai avansați furnizori din punct de vedere tehnologic. Succesul Ucrainei în a-și proteja datele critice în mai multe centre din afara țării oferă

[24] Diferite servici de procesare de date, stocare, etc ce sunt disponibile prin intermediul internetului
[25] European Union Agency for Cybersecurity

dovezi puternice că localizarea datelor nu este cea mai bună modalitate de a proteja împotriva atacurilor cibernetice.

Furnizorii de servicii cloud, în mare parte companii din SUA, se tem că schimbările ar putea fi folosite pentru a-i ține departe de piața europeană, ceea ce ar submina, la rândul său, apărarea cibernetică a continentului. Într-un articol din septembrie 2022, Google a cerut Europei să-și regândească abordarea și să-și retragă ecosistemele închise, zidurile digitale sau localizarea datelor în favoarea a ceea ce a numit „securitate deschisă", bazându-se pe parteneriate public-privat, partajarea amenințărilor și criptare în detrimentul certificării.

În această perspectivă lucrurile sunt încă neclare referitor la care parte are cu adevărat dreptate, care sunt intențiile și motivațiile reale și care ar fi cea mai eficientă modalitate de a merge mai departe pe viitor.

La nivel global există diferențe notabile între modul în care guvernele diferitelor super-puteri s-au poziționat. De exemplu, ne putem uita la Statele Unite care abordează problema securității cibernetice ca fiind o problema de securitate naționala și în consecință poate și acționează ca atare, iar, Europa pune accentul pe protejarea intimității și securității datelor personale fără a pierde din vedere obiectivul principal si anume de apărare a intereselor sale economice [38]. Pentru a înțelege anvergura daunelor, conform estimărilor efectuate de către Comisia Europeană, „factura" pe care o plătește Europa anual atunci când vine vorba de criminalitatea cibernetică este de aproximativ 5.5 miliarde euro [40].

Ce este cu clar, prin prisma multiplelor incidente și conflicte armate la nivel global, este faptul că Europa trebuie să își extindă cooperarea cu Statele Unite. În cadrul Consiliului UE-SUA pentru Comerț și Tehnologie, reprezentanții ambelor tabere au concluzionat că securitatea cibernetică trebuie făcută a fi prioritară.

Cu toate acestea, Uniunea Europeană și Statele Unite se mișcă la viteze diferite. Pe măsură ce Uniunea Europeana se grăbește cu planurile sale cibernetice, reglementările cibernetice din SUA rămân rudimentare. În urmă cu un deceniu, Camera de Comerț a SUA a condus o campanie de blocare a legislației care ar fi impus cerințe de securitate cibernetică afacerilor private. De atunci, SUA s-a bazat pe scheme voluntare, ordine executive și puterea de cumpărare a guvernului federal pentru a crște nivelul standardelor de securitate cibernetică, toate cu succes limitat.

Unul dintre momentele cheie pentru Statele Unite și modul în care au început să facă pași în direcția dezvoltării zonei de securitate cibernetică a fost atacul cu asupra Colonial Pipline Co. în Mai 2021. Compania este operatorul celei mai mari conducte de petrol din SUA

Deși, la finalul zilei vorbim de un atac ce nu a avut ca obiectiv o entitate guvernamentală, impactul pe care l-a avut a fost important la nivelul întregii țări prin creșterea prețurilor la pompă pentru carburant și blocaje în procesul de aprovizionare. Toate acestea având la rândul lor diferite ramificații în mare parte din industrii luând în considerare interconectabilitatea dintre acestea.

În cazul menționat, atacul a fost cauzat datorită unei divulgări de parole pentru un cont de VPN inactiv, iar, cu siguranța lipsa unui sistem MFA[26] nu a ajutat. Cumva, observăm că o bună parte din sistemele de bază pentru orice politică de securitate cibernetică au fost fie ignorate, fie expuse la vulnerabilități.

Fie că vorbim de persoane rău intenționate, hackeri, criminali cibernetici aceștia încearcă să se infiltreze în rețeaua și sistemele interne ale unei organizații pentru a cere răscumpărare, a opri/întârzia producția, a cauza daune organizaționale sau reputaționale sau în scopuri de hărțuire

[26] Multi Factor Authentification – autentificare multifactor

sau de răzbunare. În cazul atacului cibernetic Colonial Pipeline, hackerii au cerut o răscumpărare, așa că a motivația lor a fost pur monetară.

Din păcate, hackerii au o varietate de căi de exploatat, fie că este vorba de accesul de la distanță al angajaților/personalului prin VPN-uri și instrumente de partajare a desktopului (cum a fost cazul pentru Colonial Pipeline), conexiuni la distanță pentru furnizori externi terți (API-uri[27]), stocare nesigură a parolelor sau criptare a codurilor rău intenționate. . Acest lucru ridică întrebarea: „Cum vă puteți proteja împotriva acestor amenințări?"

Analizând circumstanțele producerii incidentului de la Colonial Pipeline putem observa o serie de evenimente inter-conectate. În primul rând divulgarea de parole de la care a pornit totul a fost cauzată de o serie de documente apărute pe dark web[28]. Conform unui studiu efectuat, peste 60% din scurgerile de date sunt cauzate de pierderea sau utilizarea incorecta a parolelor și de aici interesul ridicat al hackerilor. Având acest lucru în vedere, nu avem cum să nu menționăm cel mai mare eveniment de acest fel și anume RockYou2021 și colecția de peste 8,4 miliarde de parole și date de acces ce au fost furate și postate online în 2021 (atacul are în spate accesare din 2009 a RockYou prin injecție SQL și multe alte atacuri compilate) [41].

Revenind la Colonial Pipeline, pentru a putea crește nivelul de securitate se pot utiliza soluții de salvarea a parolelor și stocarea acestora în siguranță. Aceasta abordare pune la dispoziție o singură sursă pentru acreditările organizației și le găzduiește pe toate într-o singură locație care este securizată în mod ideal.

De asemenea, soluții de tip PAM[29] , împreună cu sisteme de management al credențialelor (password vault) pot să fie integrate în procedurile IT ale organizațiilor și pentru creșterea securității. Atunci când un cont PAM este creat pentru un utilizator intern, acreditările noului cont trebuie protejate - aici intervine „seiful de parole".

Când au nevoie de acces și de preluare a acreditărilor din seif, utilizatorii trebuie să parcurgă etapele din PAM, iar, trecând prin aceste etape o înregistrare a acestei activități este trecuta în jurnal. Această metodă de stocare centralizată permite resetarea acreditărilor după fiecare utilizare, ceea ce asigură o protecție avansată și permite un audit amănunțit, care poate ajuta la urmărirea oricărei activități suspecte până la sursă. Dacă ar fi fost implementate mai devreme, aceste metode ar fi putut ajuta la prevenirea expunerii parolelor Colonial Pipeline.

O a doua componentă în acest exemplu a fost dată de accesul la VPN, aceasta fiind una dintre cele mai comune metode prin care hackerii se infiltrează și obțin acces în organizații.

Din nefericire, deși are o mulțime de beneficii, VPN-ul vine la pachet si un minus important: practic este un instrument de timpul „totul sau nimic", iar, asta în zona de IT se transpune în oferirea de acces complet într-o anumite rețeaua sau deloc. Această abordare este generată din contextul că utilizatorii de VPN nu pot sa primească drepturi sau acces doar într-o anumită parte a rețelei (conform necesităților și gradului de acces), iar, granulația drepturilor este aproape imposibilă.

Un alt potențial risc vine din perspectiva din perspectiva responsabilității terților. VPN-urile nu oferă modalități de monitorizare și auditare a activității colaboratorilor terți în cadrul rețelei, deci nu există vizibilitate asupra activității sesiunilor. Dacă se întâmplă ceva suspect, VPN-urile nu

[27] API (Application Programming Interface) – de cele mai multe ori vorbim despre o interfață software ce constă în linia de comunicare între două aplicații și include o serie de reguli de comunicare și acces
[28] Dark web – colecție de website-uri accesibile din anumite browsere de internet, capabile să păstreze activitatea pe internet anonimă și privată
[29] Privileged Access Management – soluție pentru verificarea identității pentru a preveni atacuri cibernetice

oferă un istoric acurat în ceea privește sesiunile și accesul la rețea pentru a urmări până la sursă un eventual atac.

O ultimă componentă în atacul Colonial Pipeline a fost lipsa unui sistem de MFA care ar fi prevenit ca atacatorii sa obțină acces la sisteme interne și să amenințe cu oprirea producției. Acest sistem simplu și totuși foarte eficace este utilizat ca ultima redută în fața unui potențial atacator dornic de a obține acces neautorizat.

MFA este un sistem de securitate compus din mai multe etape de verificare a identității indivizilor ce încearcă obțină acces în anumite rețele private sau la anumite documente. Un exemplu de astfel de sistem pe care-l utilizăm în mod regulat este întâlnit în cadrul cardurilor de credit – pentru a efectua o plată ai nevoie de el in format fizic și de un cod PIN[30].

Ca finalitate, a acestui atac, Statele Unite au realizat cât de aproape au fost de o nouă criză a carburanților la nivel național fiindu-le pusă în pericol distribuția pentru întreaga costă de est prin oprirea a peste 8000 de km de conducte și închiderea sistemelor forțat.

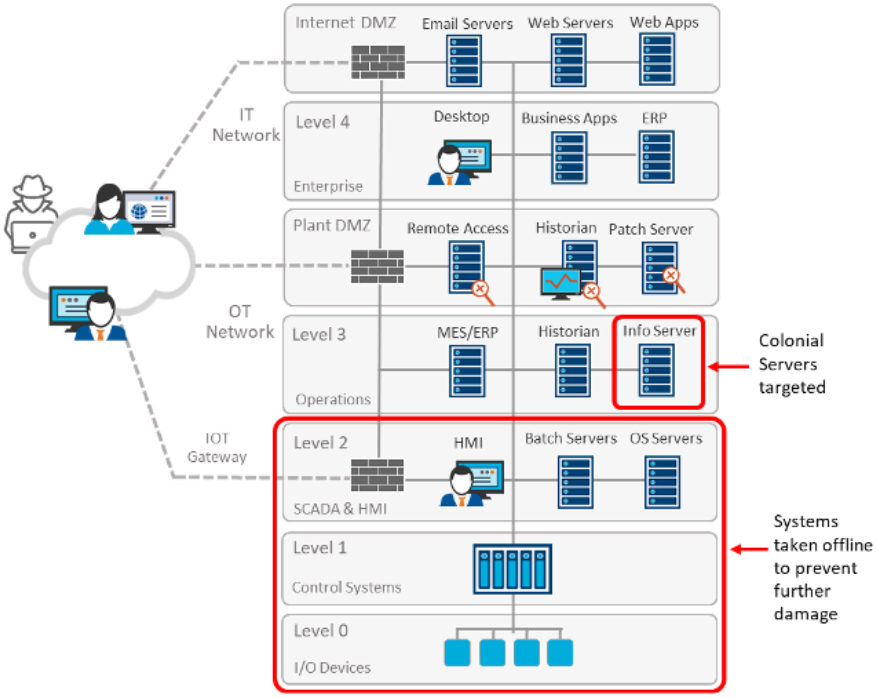


Fig. 15. Structură atac Colonial Pipelines.
Sursa: https://www.virsec.com/resources/blog/virsec-analysis-of-the-colonial-pipeline-attack

Atacul în sine fiind unul de tip ransomeware s-a închis prin transferarea sumei solicitate de gruparea Darkside și anume 4,4 mil dolari sub forma de bitcoin[31] (75 de bitcoini) - procesul fiind supervizat de către FBI. Ulterior confirmării tranzacției, un software a fost pus la dispoziția companiei pentru a prelua accesul sistemelor. Din nefericire, softul în cazul necesita un timp destul de lung pentru procesul de decriptare. În data de 7 iunie 2021, DoJ[32] a făcut o declarație publică prin care a afirmat că s-au recuperat 63,7 bitcoini în valoare de 2,3 milioane dolari (diferența fiind cauzată de fluctuațiile pieței în timpul tranzacționării) prin intermediul cheie private ale contului atacatorilor, deși nu a menționat cum a intrat in posesia acesteia.

[30] PIN – personal identification number...
[31] Bitcoin – cripto moneda ce are la bază tehologie de tip blockchain ce o face practic usor de tranzacționat și foarte dificil de urmărit
[32] Department of Justice – departamentul de justitie al statelor unite

În ceea ce privește identitatea atacatorilor lucrurile încă sunt neclare în contextul în care au fost vehiculată implicarea Rusiei în procesul de destabilizare, însă informația în cauză a fost dezmințită de către Joe Biden într-o declarație oficială [42].

Mergând pe o abordare similară de incident este inevitabil să nu aducem în discuție un virus care a făcut ravagii în întreaga lume și anume WannaCry.

Atacul ransomware WannaCry a fost un atac cibernetic la nivel mondial care a avut loc în mai 2017. Atacul cibernetic a vizat computerele care rulează Windows. Atacatorii au criptat datele și au cerut o răscumpărare, dacă aceasta nu a fost plătită, grupul a amenințat că va elibera date/informații. Microsoft a fost informat despre un potențial atac cu 12 luni înainte de atac și a lansat un patch de securitate[33] pentru a fi instalat pe toate dispozitivele electronice care rulează Windows.

Organizațiile care nu au instalat patch-ul atunci când au fost sfătuiți să facă acest lucru de la Microsoft au devenit apoi țintă. 200.000 de computere au fost infectate în 156 de țări ca urmare a atacului ransomware WannaCry.

Printre victimele atacurilor s-au enumărat NHS[34], Telefonica, America's FedEx, German railway company Deutsche Bahn, LATAM Airlines și mulți alții.

Ca abordare, pentru a beneficia de o cheie de decriptare, victimele erau puse să plătească o răscumpărare de 300 de dolari (mai târziu această sumă a crescut la 600 de dolari) sub forma de Bitcoin. Atacul ransomware WannaCry și-a avertizat victimele că fișierele lor vor fi șterse ireversibil dacă nu plătesc răscumpărarea în trei zile.

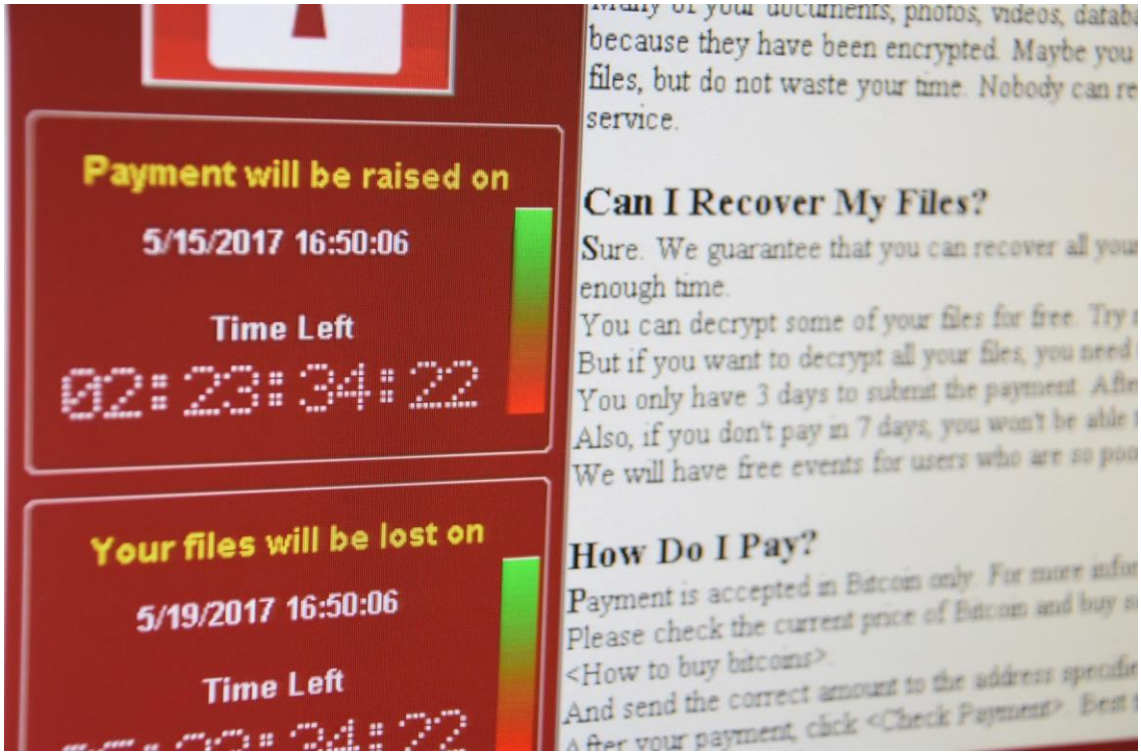


Fig. 16. Mesaj WannaCry.
Sursa: https://www.nationalhealthexecutive.com/articles/wannacry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-were-cancelled.

[33] Path de securituate – update ce are menirea de a „acoperii" anumite breșe de securitate sau erori
[34] National Health Service – sistemul național de sănătate din UK este unul dintre cele mai mari din lume după Brazilian Sistema Único de Saúde

Din perspectiva atacului, deși inițial s-a crezut că acesta a fost răspândit prin intermediul phishing-ului[35], s-a descoperit ulterior că de fapt a fost utilizată o vulnerabilitate de tip backdoor[36]

Vineri, 12 mai 2017, NHS a fost blocat timp de câteva zile din cauza WannaCry, care a afectat spitalele și cabinetele de medicilor de familie din Anglia și Scoția. Deși NHS nu a fost vizat în mod specific, atacul cibernetic global a evidențiat vulnerabilități de securitate și a dus la anularea a mii de întâlniri și operațiuni, împreună cu relocarea frenetică a pacienților din centrele de urgență afectate. De asemenea, personalul a fost forțat să revină la creion și hârtie și să-și folosească propriile telefoane mobile după ce atacul a afectat sisteme cheie, inclusiv telefoanele.

Ransomware-ul WannaCry a expus o vulnerabilitate specifică Microsoft Windows, nu un atac asupra unui software neacceptat. S-a descoperit că majoritatea dispozitivelor NHS infectate cu ransomware rulau sistemul de operare Microsoft Windows 7, dar ne actaualizat, de unde și eficiența atacului cibernetic. Ransomware-ul s-a răspândit și prin internet, inclusiv prin rețeaua N3 (rețeaua de bandă largă care conectează toate site-urile NHS din Anglia), dar, din fericire, nu au existat cazuri de răspândire a ransomware-ului prin NHSmail (sistemul de e-mail NHS).

NHS Anglia a raportat că cel puțin 80 din cele 236 de trusturi au fost afectate, în plus față de 603 centre de asistență primară și alte organizații NHS, inclusiv 595 de cabinete de medici de familie. Departamentul, NHS England și National Crime Agency au raportat că nicio organizație NHS nu a plătit răscumpărarea, dar Departamentul nu știe cât de mult a costat întreruperea serviciilor NHS, deși estimările totalizează 92 de milioane de lire sterline.

Atacul a folosit Eternalblue, numele dat vulnerabilității software din sistemul de operare Windows al Microsoft, și funcționează prin exploatarea Microsoft Server Message Block 1.0. SMB[37] este un protocol de partajare a fișierelor în rețea și „permite aplicațiilor de pe un computer să citească și să scrie în fișiere și să solicite servicii” care se află în aceeași rețea.

În mod ironic, se presupune că a fost dezvoltat ca o exploatare de atac cibernetic de către NSA a Statelor Unite. Deși s-a raportat că știau despre vulnerabilitățile instrumentului, NSA nu l-a adus în atenția Microsoft până când grupul de hackeri numit Shadow Brokers a scurs EternalBlue pe un site obscur.

O analiză ulterioară a atacului de către companii precum Symantec a dezvăluit legături cu grupul Lazarus care, la rândul său, a fost legat de Coreea de Nord, deși atacul nu poartă semnele distinctive ale unei campanii de stat național

Atacul cibernetic a fost descoperit accidental de Marcus Hutchins (la rândul său condamnat pentru dezvoltarea Kronos, un soft ce fura datele de acces în conturile bancare prin intermediul browser-ului [43]).

Un cercetător în securitatea computerelor, prin înregistrarea unui domeniu pe care ransomware-ul a fost programat să îl verifice. În săptămâna următoare, kill switch-ul a devenit ținta unor rețele botnet[38] puternice, care sperau să elimine domeniul și să declanșeze un alt focar [44].

Am adus în discuție o serie de atacuri care deși puteau să aibă impact catastrofal în ceea din perspectiva pierderilor materiale și chiar umane, trebuie subliniat faptul că ce au avut în comun aceste atacuri a fost obiectivul final și anume colectare de resurse financiare și nimic altceva.

---

[35] Pishing – tip de atac ce bazează fie pe email-uri sau pe clone de site-uri astfel încât utilizatori sunt determinați să instaleze sau să se autentifice, astfel fiindu-le periclitate datele de acces

[36] Backdoor – virus de tip malware ce permite accesul neautorizat pe un anumit sistem

[37] SMB - Server Message Block

38 Botnet – grup de computere controlate prin intermediul malware de către actori rău intenționați

De asemenea, putem scoate în evidență cazuri în care obiectivul atacului a fost centrat pe scoaterea din funcțiune a serverelor și blocare completă a activităților. Cazul la care facem referință este cel atacului DDoS asupra Sony Play Station Network efectuat de gruparea de hackeri LulzSec.

Totul a început în 2009 în contextul în care George Hotz, un cunoscut hacker a încercat și reușit pentru o scurtă perioadă de timp să spargă sistemele de securitate și să ofere utilizatorilor Play Station 3[39] o funcționalitate ce era disponibilă pe versiunile precedente: rularea de sisteme de operare alternative (în cazul de față era vorba de Linux). Ulterior unui patch, acesta portiță identificată a fost închisă și George Hotz s-a retras din activitate.

La început de 2011, cu ajutorul Alexander Igorrenknov, au reușit să spargă din nou măsurile de securitate impuse pe același sistem. Drept urmare, în Januarie 2011, Sony a depus o le-a intentat un proces iar cei doi au fost reținuți. În Aprilie gruparea Anonymous s-a implicat în poveste și a lansat un avertisment către Sony.

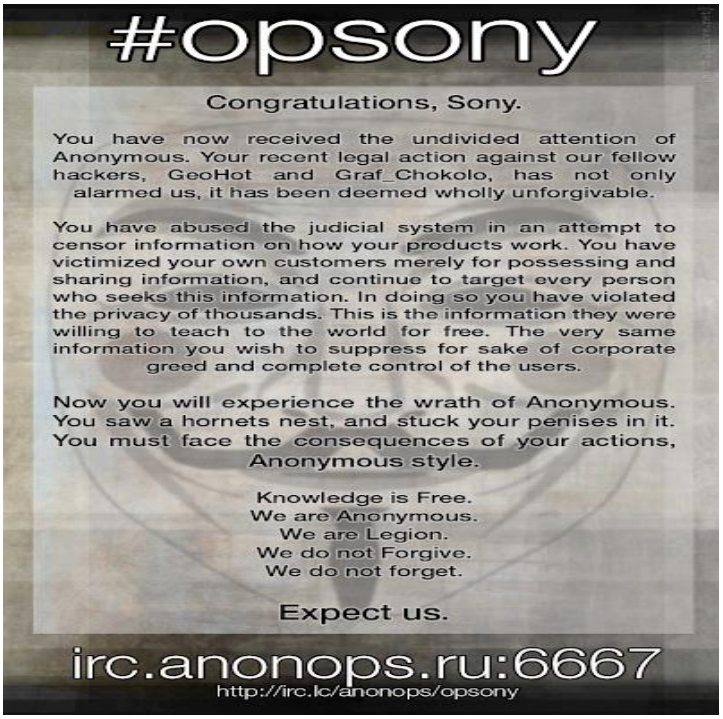


Fig. 17. Mesaj avertizare Anonymous.
Sursa: https://thehackernews.com/2011/04/operation-payback-next-target-opsony-by.html.

Anonymous a efectuat atacuri cibernetice împotriva serverelor Sony timp de trei zile. Întreruperea a fost cunoscută sub numele de „#opSony". Obiectivul operațiunii Sony a fost să facă tot posibilul pentru a submina operațiunile Sony. Pe 7 aprilie, Anonymous și-a oprit atacul. Anonymous și-a dat seama că dăuna mai degrabă consumatorilor decât Sony.

Așa că au decis să renunțe. „Anonymous nu atacă PSN în acest moment." a declarat grupul. „Ne-am dat seama că vizarea PSN nu este o idee bună. Prin urmare, ne-am suspendat temporar acțiunea până când se găsește o metodă care nu va afecta grav clienții Sony.

Anonymous este de partea ta, susținând drepturile tale." Serviciul PSN normal a fost reluat după aceea. Dar în dimineața zilei de 19 aprilie, PSN era din nou blocată. Dar Anonymous nu a fost responsabil pentru închidere. Era Sony. Două zile mai târziu, Sony a trecut din nou serverele PSN offline. „După cum știți fără îndoială, întreruperile actuale de urgență continuă în această după-amiază și toate serviciile de rețea online Sony rămân indisponibile"

[39] Play Station 3 – consolă de jocuri realizată de Sony

Sony și-a avertizat consumatorii că ar putea fi o zi întreagă sau mai mult timp de nefuncționare, chiar a doua zi, Sony a anunțat într-un comunicat de presă că a existat o „intruziune externă" în sistemul lor, care a afectat atât utilizatorii PlayStation Network, cât și Curiosity Services și a recunoscut că au dezactivat PSN pe 20 aprilie.

PSN a rămas offline încă o săptămână, ceea ce a provocat indignare din partea clienților care nu erau siguri de ce se întâmplă. Dar Sony a apărut, anunțând ceea ce urma să fie o breșă masivă de securitate care a afectat 77 de milioane de utilizatori. „Deși încă investigăm detaliile acestui incident, credem că o persoană neautorizată a obținut următoarele informații furnizate. Numele, adresa, țara, adresa de e-mail, data nașterii, parola și autentificarea PlayStation Network și ID-ul online PSN.

De asemenea, este posibil ca datele dvs. de profil, inclusiv istoricul achizițiilor și adresa de facturare și răspunsurile dvs. de securitate pentru parola PlayStation Network Curiosity, să fi fost, de asemenea, obținute." A spus gigantul corporativ. PlayStation Network a rămas offline. Sony a adus o firmă de securitate pentru a investiga încălcarea. De asemenea, efectuați actualizări ale serviciilor.

Grupul de hackeri LulzSec și-a asumat responsabilitatea pentru atac într-un final. „Fiecare fragment de date pe care l-am luat nu a fost criptat. Sony a stocat un milion de parole ale clienților săi în text simplu. Ceea ce înseamnă că era doar o chestiune de timp să o luăm." Sony a negat afirmațiile. Dar mai târziu, LulzSec a încărcat un fișier de 5 MB care descrie modul în care a fost efectuat hack-ul prin metode foarte simple de injectare.

În septembrie 2011, FBI a anunțat că a făcut arestări în atacul de la Sony Pictures. Doi membri ai LulzSec au fost arestați și acuzați. Mai multe instituții de știri au susținut că forțele de ordine au făcut arestări în hack-ul Sony [45].

Este inevitabil și lesne de observat că acest fenomen al atacurilor cibernetice a căpătat amploare în ultimii ani, și cu siguranță o să urmeze să crească si mai mult. Nu aș vrea să se înțeleagă greșit că ar este o abordare acceptată, însă as vrea să subliniez că este un simptom inevitabil al procesului de digitalizare prin care omenirea a trecut.

Da, consider că este imperios necesar ca toți actorii principali la nivel de mondial au nevoie să își actualizeze cunoștințele, să crească nivelul de vigilență instituind proceduri și reglementări care să fie capabile să țină sub control atacuri ca cele prezentate mai sus.

Din nefericire, având de-a face cu multiple forțe și arii de interes divers, ne putem găsi în situația în care să nu existe aliniere la nivel strategic și de aici pot genera o mulțime de probleme. Însă, consider că mediu privat are datoria de a fi receptiv și deschis la comunicare, iar, în egală măsură guvernele și factorii politici trebuie să conștientizeze că nu pot controla totul prin legi, ba mai mult se pot expune inutil daca nu cresc nivelul de colaborare intre state.

Foarte probabil ca războaiele viitorului să își mute teatrele de luptă din lumea reală în cea virtuală și aici fac referire la atacurile și abordările de gherilă utilizate în acest domeniu de anumite state. Nu mai este un secret că se investesc sume colosale în pregătirea acestor „trupe" sau „comandouri" digitale, iar efectele acestor atacuri pot să fie inimaginabile cu efecte și daune în viața tuturor.

Din această perspectivă responsabilitatea cade pe umerii tuturor de ne pregăti, de a înțelege care sunt riscurile și cel mai important cum le putem mitiga în așa fel încât să scădem gradul de expunere pe care-l avem, indiferent de postura în care suntem.

3.2. Tehnologia blockchain

Un blockchain este o listă de înregistrări numite blocuri care sunt legate între ele folosind mecanisme criptografice, fiecare bloc conține o valoare hash, parola, marcajul de timp și datele tranzacției din blocul anterior.

Marca temporală dovedește că datele tranzacției existau atunci când blocul a fost publicat, deoarece fiecare bloc nou conține informații despre blocul anterior, se formează un lanț în care fiecare bloc adăugat își verifică blocul anterior. Prin urmare, este extrem de dificil să schimbi datele din blockchain, deoarece odată înregistrate, acestea nu pot fi modificate fără a modifica toate blocurile ulterioare [57].

Tehnologia Blockchain încorporează multe concepte de bază (Dumitrache, 2022), nodurile sunt cele mai de bază elemente ale blockchain-ului. În mod logic, blockchain constă dintr-o rețea de noduri. Din punct de vedere fizic, nodurile sunt computere. O tranzacție este orice operațiune din blockchain, bunăoară pentru a modifica o valoare în blockchain, Tranzacțiile noi, pentru a fi acceptate, necesită aprobarea de cel puțin 50% +1 din nodurile existente.

În blockchain, datele sunt stocate în blocuri, fiecare din aceste blocurile sunt legate de blocul anterior printr-un hash criptografic. Un cont blockchain este format din două variabile, cheie privată și cheie publică. Contul aparține deținătorului cheii private. Ajunge, spre deosebire de alte tehnologii centralizate, în blockchain nu există nicio procedură de recuperare a parolei dacă se pierde cheia private (Dumitrache, 2022).

Principalele caracteristici ale blockchain-ului sunt:

- Descentralizare – Datele sunt reținute în mai multe locații din rețea, egal cu numărul de noduri;
- Autonome – Nu există o organizație sau agenție centrală care să gestioneze blockchain-ul și să dețină cheile pentru corectarea datelor;
- Auditabilitate – Deoarece fiecare bloc este legat de blocul anterior printr-un hash, toate modificările pot fi urmărite cronologic;
- Funcționare continuă – Datele din sistem sunt replicate pe mii de computere simultan, astfel încât să poată fi utilizate chiar dacă 99% dintre computere sunt offline;
- Scalabilitate – O rețea poate conține un număr nelimitat de noduri;
- Securitate – Codul sursă folosit este open source și nu a fost niciodată scurs;
- Scalabilitate – Codul permite dezvoltarea de noi servicii și produse;
- Securitate – Pentru a aproba o tranzacție, mai mult de jumătate dintre nodurile din rețea trebuie să accepte tranzacția.

Dacă un atacator reușește să modifice părți ale blockchain-ului sau ale datelor, este creat un nou bloc care trebuie verificat de toate dispozitivele din rețeaua blockchain. Pentru a accepta tranzacții frauduloase, jumătate dintre noduri plus un nod trebuie schimbate, și toate nodurile trebuie schimbate simultan. Dacă răspunsul unui nod este diferit de hash-ul criptografic al altui nod este verificat, și nodul este ignorat de rețea până când revine la versiunea adevărată a datelor (Dumitrache, 2022).

Nick Szabo definește conceptul de „contracte inteligente” ca o posibilă modalitate de a formaliza relațiile de afaceri și acordurile comerciale într-un mediu online, într-o manieră mai eficientă decât contractele tradiționale pe hârtie (Dumitrache, 2022).

Contractele inteligente sunt contracte digitale care se execută automat, care necesită ca două entități să îndeplinească sarcini pentru a iniția o tranzacție. În blockchain, astfel de contracte nu pot fi modificate de nicio parte, iar termenii lor sunt monitorizați în mod continuu pe măsură ce se parcurg pașii necesari pentru implementarea acestuia.

Dacă sunt necesare modificări, trebuie creat un contract complet nou, contractele inteligente sunt mici programe, identificate printr-o adresă și stocate în blockchain ca orice altă tranzacție, care se execută automat când sunt îndeplinite condițiile predefinite. Codul sursă al contractului este scris într-un limbaj de programare specific, cum ar fi Solidity, un limbaj de nivel înalt orientat pe obiecte dezvoltat pentru modelul Ethereum Virtual Machine (Dumitrache, 2022).

3.3. Serviciile de e-Guvernare și contextul european

Tranziția la sistemele de guvernare electronică are consecințe importante pentru cetățeni și organizații, sistemele de guvernare electronică necesită stocarea, și schimbul de date în formă digitală.

Guvernele mențin centre de date vaste pentru a stoca informații sensibile precum: identitate, venituri, dosare medicale etc. Sistemele informaționale trebuie să implementeze mecanisme de securitate adecvate pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor (Dumitrache, 2022).

Datele personale sunt adesea pierdute din cauza erorilor în proiectarea și implementarea sistemelor tehnice și a adoptării insuficiente a măsurilor de securitate. E-guvernarea este un efort guvernamental de a automatiza serviciile publice, și de a facilita utilizarea acestora de către cetățeni. Comisia Europeană recunoaște nevoile cetățenilor, întreprinderior și a guvernelor, în acest sens a fost elaborat un plan de acțiune pentru următorii zece ani [57].

Comisia Europeană propune patru direcții principale pentru a transpune ambițiile digitale ale UE pentru 2030 în obiective concrete, și pentru a se asigura că acestea sunt atinse:

- Populație cu competențe digitale și profesioniști pregătiți corespunzător;
- Infrastructură digitală durabilă, sigură și de înaltă performanță;
- Transformarea digitală a întreprinderilor și a întreprinderilor va depinde de capacitatea acestora de a adopta rapid noi tehnologii digitale, inclusiv în cadrul ecosistemelor industriale și de servicii;
- Digitalizarea serviciilor publice pentru a oferi servicii publice online tuturor cetățenilor, oferind servicii și instrumente cu standarde ridicate de securitate și confidențialitate.

Obiectivele pentru 2030 stabilite de Comisia Europeană, includ construirea unei infrastructuri paneuropene pentru procesarea datelor comune interconectate, dezvoltarea capabilitati de vârf în timp real (latență scăzută) pentru a satisface nevoile utilizatorilor finali, proiectare unei platforme middleware sigură, și interoperabilă pentru utilizare interdepartamentală, și facilitarea schimbului de date.

Sistemele blockchain pot fi implementate pe baza anumitor caracteristici, precum: numărul de beneficiari, volumul de date, domeniul de aplicare etc. În funcție de modul de implementare Blockchain este împărțit în: public, privat, și de top consorțiu.

Blockchain-urile publice permit oricui să participe la executarea și verificarea tranzacțiilor. Protocolul de consens asigură integritatea conținutului registrului. Blockchain-urile publice sunt „complet descentralizate”, și oferă cel mai înalt nivel de Securitate, exemple de blockchain publice sunt Ethereum și Bitcoin. Blockchain-urile private operează într-o rețea închisă creată de o organizație. Organizațiile au dreptul de a decide ce entități au acces de citire/scriere la blockchain. Acest model este utilizat special pentru gestionarea bazelor de date. Blockchai-ul de tip consorțiu este compus, și gestionat de mai multe organizații (părți interesate), blockchain-ul consorțiului este „semi-descentralizat”, și oferă o platformă sigură pentru tranzacțiile între organizații [57].

Algoritmul Proof of Work (PoW) necesită ca fiecare nod din rețea să rezolve probleme matematice complexe. Primului nod care rezolvă problema i se acordă permisiunea de a adăuga unul noi blcocuri, și minerii sunt recompensați pentru munca lor.

Nodul reprezintă punctul de management al blockchain-ului, și verifică legalitatea tranzacțiilor din fiecare bloc, blocul tranzacției este verificat, și datele sunt scrise în blockchain, PoW reprezintă algoritmul de consens original în rețelele blockchain.

Pe măsură ce rețeaua crește, problemele matematice complexe pe care minerii trebuie să le rezolve necesită tot mai multe resurse de calcul, și implicit consumul resurselor energetice cresc, iar rezultatele rezolvării acestor probleme se numesc hash.

Complexitatea sarcinii este o problemă sensibilă deoarece, acest lucru depinde de acuratețea și viteza scrierilor blockchain, dacă generarea blocurilor durează prea mult, tranzacția va fi blocată și se va opri executarea, iar fluxul de lucru se va opri pentru o perioadă de timp, iar dacă problema este minoră, rețeaua este vulnerabilă la atacurile DoS și Spam [57].

Modelul PoW consumă multă energie (după cum vom putea observa din graficul următor), astfel încât menținerea rețelei Bitcoin necesită o cantitate echivalentă de energie electrică consumată de o țară la fel de mare ca Argentina.

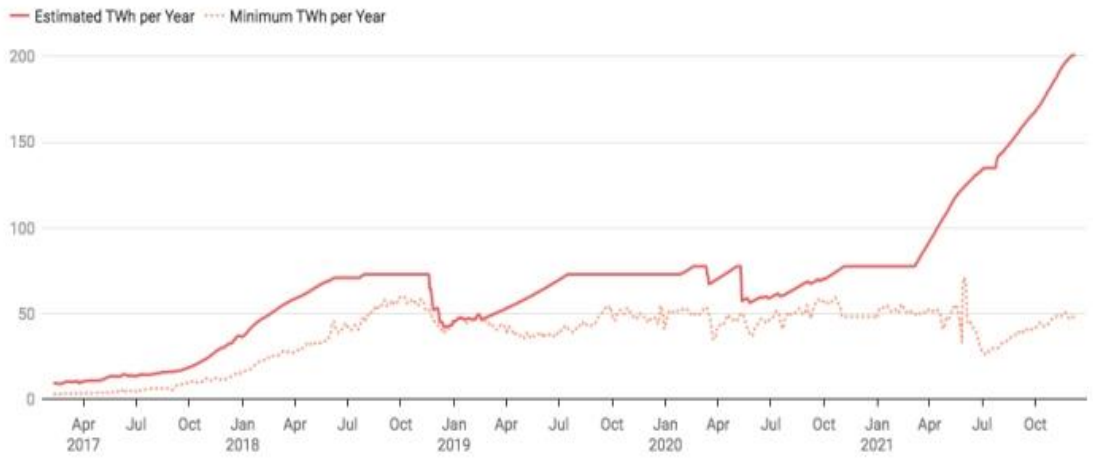


Fig. 18. Consumul anul de energie al rețelei Bitcoin.
Sursa: https://www.independent.co.uk/tech/bitcoin-energy-use-price-latest-b2110179.html.

Protocolul de consens Proof of Stake (PoS) a fost creat ca un algoritm alternativ pentru a aborda problemele de scalabilitate și sustenabilitate din jurul Proof of Work. Algoritmul PoS încearcă să rezolve problema consumului ridicat de energie din metoda PoW, prin înlocuirea efectivă a nevoii de putere de calcul cu Stake-ul, puterea de calcul a unui individ este limitată de procentul de Stake deținut.

Aceasta înseamnă o reducere semnificativă a consumului de energie. Proof of Stake (PoS) încarcă să rezolve această problem, prin alocarea puterii de minerit proporției de monededeținute de fiecare miner în parte. Cei cu resurse financiare semnificative, au în mod clar capacitatea de a miza mai multetoken-uri,și astfel de a obține mai mult control asupra rețelei, obținând în acest mod mai multe comisioane.

Cu toate acestea, sistemele PoS sunt mai puțin susceptibile de a fi centralizate, în comparație cu centralizarea blockchain-urilor PoW, unde câteva entități controlează majoritatea puterii miniere, în PoS, securitatea este mai mică decât abordarea PoW, unde un atacator în PoS ar trebui să obțină 51% din criptomoneda pentru a efectua un atac.

În ultimii ani, unele guverne au dezvoltat o varietate de soluții pentru a aplica tehnologia la diferite funcții și servicii din educație, sănătate, achiziții publice și alte domenii publice cum ar fi, securitate cibernetică, transport și managementul identității. Dar în ciuda potențialului blockchain, experimentele și cercetările arată că este nevoie de o dezvoltare suplimentară înainte ca blockchain-ul să poată fi utilizat pe scară largă în serviciile de e-guvernare.

O implementare cu succes este KSI, o tehnologie blockchain concepută în Estonia și utilizată la nivel global, care securizează rețelele și sistemele IT.
Confidențialitatea datelor, prin implementarea acestei soluții Estonia a devenit prima țară care a implementat infrastructura blockchain la nivel național (KSI Blockchain, 2021).

După valul de atacuri cibernetice din 2017, oamenii de știință estonieni au început să regândească securitatea datelor, proiectând un sistem electronic de etichetare a datelor care ar putea dovedi integritatea datelor, rețelelor și proceselor fără a se baza pe o autoritate centralizată. Inventat de Guardtime, KSI Blockchain este o alternativă masiv scalabilă la PKI, în 2020 KSI a devenit primul sistem blockchain care a primit certificarea eIDAS, marca de încredere a Uniunii Europene pentru serviciile calificate pentru tranzacții electronice în Piața Unică Europeană. (KSI Blockchain, 2021)

Prin implementarea KSI în rețelele guvernamentale estoniene, actorii rău intenționați (hackeri), administratorii de sistem sau reprezentanții guvernului nu pot manipula sau modifica date, autenticitatea lor poate fi dovedită matematic în orice moment. Autoritatea Estonă pentru Sisteme Informaționale (RIA) este furnizorul intern de servicii al guvernului, garantând agențiilor de stat accesul la rețeaua blockchain prin infrastructura X-Road. Agențiile guvernamentale folosesc SDK-uri și instrumente prefabricate pentru a implementa tehnologia blockchain. (Dumitrache, 2022).

3.4. Arhitectura generală a sistemului de e-guvernare bazat pe blockchain

Cetățenii pot accesa serviciile de e-guvernare și pot fi autentificați utilizând identitatea electronică eID combinată cu autentificarea SSI (Self Sovereign Identity), disponibilă prin telefon mobil sau printr-o aplicație dedicată.

Procesul de autentificare în sine este o tranzacție înregistrată în blockchain, după conectarea cu succes, selectați un serviciu public din lista de servicii disponibile, cum ar fi plata taxelor de studii, și aceștia să fie redirecționați către formularul electronic de plată, unde introduc numele instituției de învățământ, suma și obiectul plății (bunăoară taxe de studii master) și datele cardului bancar.

Plata este procesată cu success și se primește o confirmare electronică prin e-mail, operațiunea este înregistrată ca tranzacție în blockchain, pe baza unui contract inteligent (smart contract) între instituția de învățământ și serviciul plăti care confirmă plata taxei, ulterior tranzacția este salvată în blockchain. Pot fi definite contracte inteligente, cetățean cu cetățean, instituție cu instituție, și cetățean cu o instituție [57].

Nivelul ridicat de securitate al tehnologiei blockchain este un avantaj față de alte instrumente și tehnologii utilizate în tranzacțiile și procesarea datelor, datorita combinatiei între criptografie și rețeua distribuită, implementările bazate pe blockchain produc un registru imuabil și inviolabil al tranzacțiilor confirmate și autentificate.

Avantajele unui astfel de ecosistem sunt securitatea ridicată, transparența și trasabilitatea tranzacțiilor, dacă într-un sistem clasic documentele pot fi pierdute sau deteriorate, într-un sistem digital bazat pe tehnologia blockchain, probabilitatea pierderii globale a datelor este mica (Dumitrache, 2022).

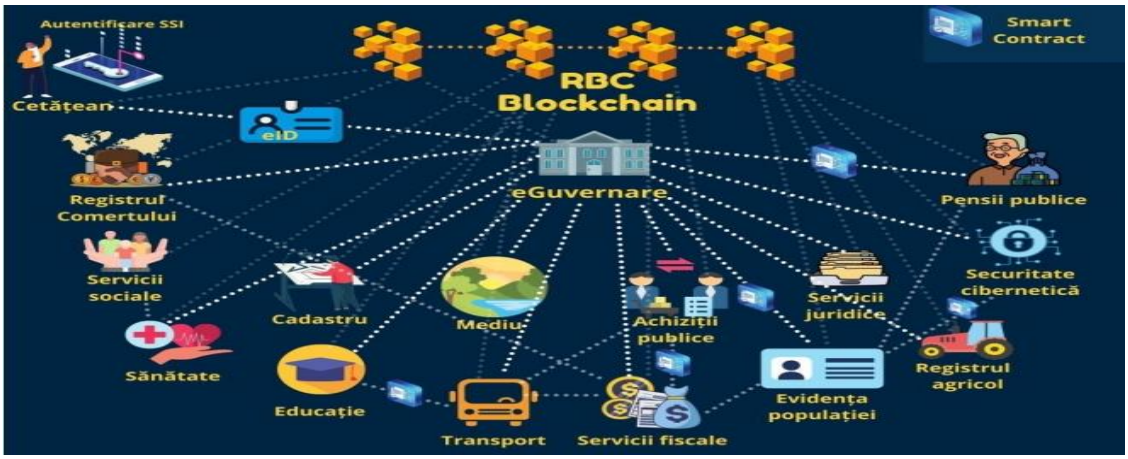


Fig. 19. Arhitectura generală a sistemului de e-guvernare bazat pe blockchain.
Sursa: https://www.researchgate.net/figure/Figura-4-Model-conceptual-Blockchain-pentru-servicii-de-eGuvernare_fig3_359088197.

Un ecosistem de guvernare electronică care utilizează blockchain oferă diverse avantaje, cum ar fi:

- Descentralizare;
- Tranzacții sigure și securizate;
- Scalabilitate;
- Eficiență;
- Costuri reduse de sincronizare a datelor;
- Interoperabilitate.

3.5. Bune practici și politici pentru prevenirea și limitarea atacurilor cibernetice

În cee ace privește componentele hardware și software ale internetului , acestea sunt utilizate pentru a desfășura afaceri, și a transfera informații între diverse entități, inclusiv companii, organizații și agenții guvernamentale către consumatori. Capacitatea de a fi vulnerabilă la atacurile cibernetice, nu sunt doar împrejurimile fizice, dispozitive mobile, computere, smartphone-uri etc.

Cu toate acestea, același lucru este valabil și pentru abordarea logică, sisteme de operare, aplicații, e-mail, și transfer de informații între companii sau în cloud. În urma unui sondaj realizat, care include majoritatea incidentelor (hardware și software) din instituțiile publice din România, sunt asociate cu echipamente fixe (38%), e-mail (25%), și aplicații Web (17%) [58].

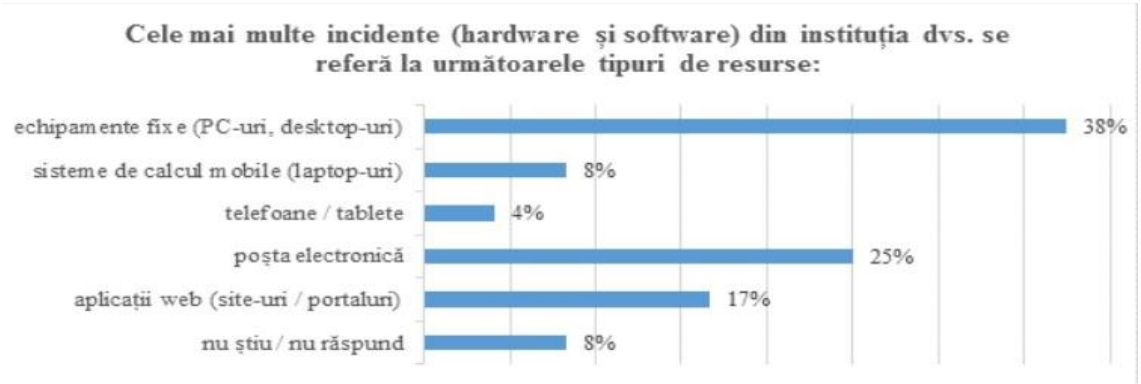


Fig. 20. Chestionar cu privire la incidentele (hardware și software), care au fost întâlnite cel mai des în cadrul instituțiilor publice din România.
Sursa: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf.

Aceste atacuri au crescut atât în volum, cât și în complexitate, ceea ce a dus la creșterea riscului, costuri suplimentare și pierderi potențiale pentru companii. Instituțiile specializate în special pe piețele financiare și de capital, sunt atractive datorită volumului tranzacțiilor lor pe aceste piețe, și a datelor care sunt vehiculate, cum ar fi informații despre clienți (prezenti și potențiali), baze de date (inclusiv informații din trecutul lor), planuri de afaceri, strategii și investiții confidențiale, proprietate intelectuală (cum ar fi algoritmii de tranzacționare), portofolii de clienți sau liste de utilizatori, precum și parole [58].

Progresele tehnologice au facilitat procedurile și procesele simplificate, și au permis instituțiilor să utilizeze noi metode care le permit să-și comunice mesajele, și să aibă o gamă mai largă de opțiuni de comunicare, și un serviciu mai flexibil și mai eficient.
În schimb, prevalența tot mai mare a acestor instrumente a condus la creșterea riscului de atacuri cibernetice, scopul principal al acestor atacuri este de a fura date:

- Aceste atacuri având un impact negativ asupra funcționării (întreruperea, blocarea, distrugerea sau controlul ilegal al unui sistem informatic sau a infrastructurii informaționale);
- Încălcarea confidențialității, încrederii și accesibilității datelor, sau sistemelor IT din instituții;
- Impact asupra autenticității datelor, și sustragerea de informații care sunt restricționate.

Aceste atacuri sunt comise de numeroase tipuri de agenți (organizații criminale, autori individuali, oficiali guvernamentali, teroriști, angajați nemulțumiți, concurenți etc), din diverse motive, dintre care cele mai semnificative sunt:

- Beneficii bănești;
- Furtul, constrângerea sau modificarea datelor;
- Dobândirea de beneficii superioare, și informații secrete de la concurență;
- Distrugerea organizației vizate, sau dezvăluirea unor informații în scop de răzbunare.
- Susținerea principiilor politice și/sau sociale;
- Practica terorii, răspândirea panicii și haosul [58].

Hackerii au mai multe metode de atac disponibile, dintre care pe cele mai comune le vom enumerate mai jos:

- Malware - instalarea de programe dăunătoare, care afectează negativ funcționalitatea computerelor și a comunicațiilor.
- Ingineria socială - este o metodă de înșelăciune care presupune obținerea de informații personale care sunt confidențiale, precum parole, date personale și carduri bancare.
- Atacurile DDoS - care sunt menite să împiedice accesul sau să întârzie livrarea serviciilor, sau la sistemele unei organizații.
- Botnets - autorii sunt dintr-o retea sau dintr-un numar mare de computere infectate, care sunt folosite pentru a trimite spam sau virusi, sau pentru a inunda reteaua cu mesaje, acest lucru duce la blocarea serviciului;
- Advanced Persistent Threats (APT) - sunt atacuri cibernetice complexe, care utilizează cunoștințe și instrumente pentru a recunoaște, și pentru a exploata deficiențe tehnologice specifice.

Orice organizație poate deveni victima unui atac cibernetic, natura amenințării cibernetice depinde de tipul, vulnerabilitățile și informațiile sau activele organizației. Efectele lor pot fi semnificative în ceea ce privește reputația organizației, pierderea financiară sau pierderea avantajului competiti.

În timp ce gradul în care impactul depinde de detectarea și răspunsul rapid după atac este recunoscut. Unele dintre cele mai eficiente metode de securitate cibernetică pentru instituțiile publice din România sunt enumerate mai jos [58].

1. Examinarea aplicațiilor care au acces la date:

Aplicațiile web pentru organizații oferă instrumentele necesare pentru funcționalitate și productivitate, dar pot pune, de asemenea, în pericol datele cruciale. protejarea informațiilor critice necesită, de obicei, instalarea unui software firewall și crearea unei infrastructuri în jurul datelor care sunt protejate. Programele firewall trebuie proiectate cu prudență, doar aplicațiile autorizate având acces la date confidențiale sau care scriu.

2. Crearea controalelor individuale de acces:

Prin crearea unor reguli de autorizare specifice pentru fiecare utilizator, aceştia pot restricționa accesul doar la sistemele de care au nevoie pentru sarcinile de serviciu, acest lucru va împiedica expunerea datelor personale care sunt sensibile.

3. Achiziția de loguri individuale cu detalii specific:

Pentru un raport cuprinzător al ceea ce se întâmplă în sistemele din rețeaua companiei, atât pentru securitate, cât și pentru depanare, trebuie adunate jurnalele detaliate și rapoarte complete. Acest lucru este valabil mai ales pentru aplicațiile care nu au înregistrări interne, astfel încât orice posibile breșe de securitate cauzate de aceste aplicații pot fi urmărite și remediate.

4. Menținerea actualizărilor de securitate:

Infractorii cibernetici dezvoltă mereu noi metode de atac și încearcă să găsească noi puncte slabe, ca urmare, pentru a proteja rețeaua de calculatoare, trebuie utilizate cele mai recente semnături antivirus sau patch-uri anti-malware.

5. Evitarea ingineriei sociale:

Securitatea implementată la un nivel tehnic este vulnerabilă la erorile umane, metoda de inginerie socială a fost folosită cu succes de zeci de ani pentru a obține informații de conectare, și acces la fișierele protejate prin parolă.
Aceste tipuri de încercări pot apărea prin e-mail, telefon sau alte metode de comunicare cuutilizatorii.

6. Educarea și pregătirea utilizatorilor:

Utilizatorii sunt de obicei cea mai slabă componentă a sistemului de securitate a informațiilor, iar acest lucru poate fi atenuat prin predarea continuă despre cele mai bune metode de securitate cibernetică. Instruirea ar trebui să acopere modul de a recunoaște un e-mail fals, de a crea parole puternice, și de a evita aplicațiile dăunătoare, de a menține informațiile interne ale companiei, și orice alte pericole asociate cu securitatea cibernetică.

7. Descrierea clară a politicilor de utilizare în cazul noilor angajați:

Pentru a consolida și clarifica îndatoririle de instruire ale utilizatorilor, cerințele și așteptările companiei cu privire la securitatea IT ar trebui documentate la angajare, (contractele de muncă trebuie să aibă secțiuni care descriu aceste cerințe de securitate în detaliu).

8. Crearea unui plan de răspuns la o breșă de securitate:

Indiferent de gradul în care sunt respectate aceste practici recomandate, incidentele de securitate sunt așteptate și inevitabile. Acesta este motivul pentru care este important să existe un plan de răspuns la securitatea cibernetică, eliminând toate vulnerabilitățile, și minimizând daunele pe care le pot provoca atacurile cibernetice [58].

Societatea actuală este caracterizată de schimbare constantă, care necesită disponibilitatea unor comunicații globale care sunt accesibile și suficient de rapide pentru diferite clase de utilizatori. Datorită cantității fără precedent de dezvoltare software și securitate a informațiilor, securitatea informațiilor a devenit o preocupare semnificativă. Luarea deciziilor manageriale moderne este facilitată de accesul la cantități mari de informații și de o abordare distribuită a muncii.

Necesitatea utilizării și valorificării facilităților rețelelor de comunicații, impune ca securitatea și protecția informațiilor să fie o cerință obligatorie pentru orice sistem, aplicație sau serviciu. Transmiterea de informații între un expeditor și un destinatar prin internet poate avea loc prin mai multe rețele de comunicații, ceea ce permite utilizatorilor acestor rețele să intervină și/sau să modifice informațiile. De asemenea, printr-un acces neautorizat la resursele sistemului, utilizatorii din aceeași rețea cu expeditorul sau destinatarul, pot să modifice și să distrugă datele informatice.

Necesitatea securității este derivată din faptul că niciun sistem informatic nu poate fi complet sigur, singura modalitate de asigurare a siguranței este prin dezvoltarea unui sistem de Securitate, și implementarea unor mecanisme complexe de protecție care împiedică majoritatea utilizatorilor să ignore sistemul.

Din punct de vedere practic, asigurarea unui mediu sigur prin utilizarea sistemelor IT este acum o cerință obligatorie a societății, aceasta a devenit o preocupare intense, și constantă în ceea ce privește potențialele pericole și riscuri.

Baza securității informațiilor este crearea de planuri, reguli, reglementări și politici pentru a face față atacurilor care pot implica compromiterea datelor și a informațiilor. Asigurarea securității cibernetice devine din ce în ce mai complexă, acest lucru necesită implicarea mai multor niveluri de mecanisme care sunt incluse în politicile publice.

Politicile publice se caracterizează printr-o serie de decizii conexe privind scopul, mijloacele și resursele care sunt dedicate realizării unor situații particulare. Astfel, politicile publice se pot considerat un exemplu practic de abordare a problemelor din sectorul administrației publice în domeniul securității cibernetice [58].

Crearea politicilor publice privind securitatea cibernetică trebuie să urmeze o serie de principii, printre care:

- Stabilirea responsabilitatilor directe pentru definirea strategiilor si reglementarii, precum si pentru coordonarea si implementarea acestora in vederea sustinerii si promovarii deciziilor strategice.
- Pledează pentru un sistem sigur și de încredere pentru domeniul .ro;
- Crearea unui cadru formal de contractare care implică respectarea unui număr de standarde și reguli privind securitatea cibernetică;
- Măsuri funcționale referitoare la crearea unui plan de răspuns în situații de urgență, backup și continuitatea afacerii, precum și testarea regulată a vulnerabilităților.

Din perspectiva specificului domeniului securității cibernetice, politicile publice au o serie de dificultăți în asigurarea unui spațiu virtual sigur și de încredere, printre care:

- Realizarea unui studiu de impact la nivelul autorităților publice, pentru a demonstra necesitatea securității cibernetice pentru sistemele de comunicații, și tehnologia informației ca parte a infrastructurii importante.
- Colectarea de rutină a informațiilor (rapoarte, comunicări) pentru a propune noi abordări de natură reactivă sau preventivă, pentru a minimiza riscul pentru administrație.

- Organizarea politicilor publice privind securitatea cibernetică pe baza modelelor sectoriale pentru fiecare domeniu de activitate asociat instituțiilor guvernului central din România.
- Consolidarea cooperării dintre oficialii administrației publice și alte instituții și țări europene prin asistență metodologică, transfer de expertiză și bune practici [58].

O altă componentă care trebuie luată în considerare este aspectul financiar al politicilor publice, care poate oferi și un cadru consistent și organizat în ceea ce privește costurile, și investiții în securitate digitală la nivelul superior de administrație.

Lipsa estimărilor bugetare care să asigure asocierea dintre scopurile asumate și verificarea deciziilor manageriale este cauza majorității deciziilor luate cu privire la cheltuielile de teren. În funcție de sectorul de activitate și de cerințele specifice ale organizației, politicile publice privind securitatea cibernetică ar trebui inițiate și implementate la nivelul procesului de elaborare a politicilor, care are scopul de a autoriza, coordona și impune respectarea acestora, până la nivelul de execuție, fiind în mod direct responsabil de implementarea politicilor.

Cheltuielile asociate cu protejarea securității cibernetice diferă în funcție de specificul domeniului de activitate (complexitatea fluxurilor, dimensiunea sistemelor informatice, numărul utilizatorilor atât publici cât și privați etc.), dar și semnificația și criticitatea infrastructurii în domeniul respectiv.

Implementarea politicilor publice privind securitatea cibernetică și managementul operațional va facilita o mai bună înțelegere a dificultăților asociate domeniului și va oferi resursele necesare pentru a modifica modul în care este modelată managementul amenințărilor în spațiul cibernetic. De asemenea, permite o estimare precisă a eforturilor tehnice și non-tehnice necesare implementării măsurilor practice în domeniul securității cibernetice [58].

Concluzii

După cum am putut observa din prezenta lucrare, atacurile cibernetice au început să aibă în ultimii ani o creștere dramatică a diversității, unele dintre acestea sunt considerate a fi "o adevărată epidemie la nivel global", și care au o rată mare de propagare în mediu virtual.

Amenințările specifice sistemelor informaționale au o dinamică mai proeminentă și o natură universală, ceea ce face dificilă recunoașterea și apărarea împotriva acestora. În ciuda faptului că sunt disponibile multe metode de protecție, eficacitatea lor este în creștere, așa cum este și cazul securității informației în spațiul cibernetic, care nu poate fi realizată numai prin mijloace tehnice, în primul rând o problemă umană

De multe ori, incidentele legate de securitate sunt cauzate de organizarea insuficientă a politicii de securitate, și lipsa de diligență a mecanismelor de securitate. În acest context este importantă dezvoltarea strategiilor de securitate cibernetică, prin crearea de politici în acest sens și campanii de prevenire, și eradicare a fenomenului criminalității informatice la nivel național.

Odată cu progresul tehnologiei blockchain în alte domenii decât cel al criptomonedelor, volumul cercetărilor dedicate tehnologiei a crescut semnificativ în ultimii ani. Tehnologia blockchain este considerată a fi o metodă de abordare care revoluționează serviciile publice și e-guvernarea, și funcționează ca un facilitator pentru cetățeni, întreprinderi și guvern pentru a interacționa într-un mod transparent.

Tehnologia blockchain reprezintă rezultatul unei combinații de transparență, onestitate, confidențialitate și responsabilitate care este concepută corect. Rețea blockchain împreună cu natura sa bazată pe încredere, a condus la o creștere a încrederii tuturor participanților, deoarece tranzacțiile sunt efectuate în siguranță, fără ingerința autorităților centrale.

Blockchain-ul din punct de vedere al tehnologiei are potențialul pe cât posibil de a contribui în mare măsură la crearea unor servicii de e-guvernare transparente și sigure, În perioada următoare, este necesară o cercetare sporită în domeniu pentru a proiecta servicii practice de e-Guvernare care utilizează tehnologia blockchain.

După cum am văzut anterior protocoalele PoW și PoS, a demonstrat o implementare cu succes a unui blockchain în domeniul e-Guvernării, și a creat un design general
bazat pe blockchain, contracte inteligente, precum și ID-uri dedicate serviciilor de e-Guvernare.

În viitorul apropiat, se preconizează că tehnologia blockchain va copleși, schimba și îmbunătăți metoda actuală de bussines, de guvernare etc, contractele inteligente vor facilita automatizarea proceselor, digitalizarea fiind următorul pas în buna funcționare a administrației și al instituțiilor publice.

References

[1] F. Heady, Public Administration. A Comparative Perspective, Boca Raton: CRC Press, 2001.

[2] L. Radu, „Elemente de istorie a administrație publice (partea I),” *Revista Transilvană de Ştiinţe Administrative,* vol. 1, nr. 47, pp. 88-89, 2020.

[3] D. Georgakakis, „The deconsecrated administration: EU civil servants from mission to management,” *HAL Open Science,* 2022.

[4] OECD Publications, „Public Sector Leadership for the 21st Century,” 2001. [Interactiv]. Available: https://read.oecd-ilibrary.org/governance/public-sector-leadership-for-the-21st-century_9789264195035-en#page1. [Accesat 21 1 2024].

[5] OECD, „Instrumente juridice ale OCDE,” [Interactiv]. Available: https://legalinstruments.oecd.org/api/download/?uri=/public/af1338f9-ac4f-4b19-8d64-ad749e3aa587.pdf. [Accesat 21 1 2024].

[6] F. Negoiță, Istoriei administraţiei publice, București: Universul Juridic, 2011.

[7] M. Matthias, „Encyclopaedia Britannica,” 16 1 2024. [Interactiv]. Available: https://www.britannica.com/money/topic/Industrial-Revolution/The-first-Industrial-Revolution. [Accesat 23 1 2024].

[8] C. Vrabie, Elemente de E-guvernare, București: Pro Universitaria, 2014.

[9] M. Maciejewsk, „To do more, better, faster and more cheaply: using big data in public administration,” *International Review of Administrative Sciences,* vol. 83, nr. 120, 2017.

[10] J. Reis, P. E. Santo și N. Melão, „Impacts of Artificial Intelligence on Public Administration: A Systematic Literature Review,” *Iberian Conference on Information Systems and Technologies (CISTI),* 2019.

[11] „Directive on Measures For a High Common Level of Cybersecurity Across the Union (NIS2 Directive),” European Commission, 16 1 2023. [Interactiv]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive. [Accesat 6 1 2024].

[12] „NIS Cooperation Group,” European Commission, 7 6 2022. [Interactiv]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group. [Accesat 6 1 2024].

[13] „Questions and Answers – Eu Cybersecurity,” European Commission, 26 6 2019. [Interactiv]. Available: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369. [Accesat 6 1 2024].

[14] O. v. Daalen, „In defense of offense: information security research under the right to science,” *Computer Law & Security Review,* vol. 46, 2022.

[15] J. Brancolini, 5 4 2023. [Interactiv]. Available: https://cepa.org/comprehensive-reports/europe-upgrades-its-cybersecurity-arsenal-frightening-the-us/. [Accesat 22 1 2024].

[16] „Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts,” The European Parliament – IMCO & LIBE Committees, 21 4 2021. [Interactiv]. [Accesat 6 1 2024].

[17] J. Brancolini, „Europe Upgrades its Cybersecurity Arsenal — Frightening the US,” CEPA, 5 4 2023. [Interactiv]. Available: https://cepa.org/comprehensive-reports/europe-upgrades-its-cybersecurity-arsenal-frightening-the-us/#footnote_3_17314. [Accesat 6 1 2024].

[18] „New EU Cybersecurity Rules Are Well-Intended, but Introduce Unnecessary Red Tape," CCIA, 15 9 2022. [Interactiv]. Available: https://ccianet.org/news/2022/09/new-eu-cybersecurity-rules-are-well-intended-but-introduce-unnecessary-red-tape/. [Accesat 6 1 2024].

[19] J. Allen, Middle Egyptian: An introduction to the language and culture of hieroglyphs., Cambridge University Press, 2014, pp. 2-10.

[20] O. Omolara și O. I. Abiodun, „Developing a modified Hybrid Caesar cipher and Vigenere cipher for secure Data Communication. Computer Engineering and Intelligent Systems," *Computer Engineering and Intelligent Systems,* vol. 5, nr. 5, pp. 34-46, 2014.

[21] S. A. Aized, R. Irfan și R. Umair, „An enhanced vigenere cipher for data security.," *Int. J. Sci. Technol,* nr. 5.3, pp. 141-145, 2016.

[22] K. Ellison și S. Kim, A Material History of Medieval and Early Modern Ciphers Cryptography and the History of Literacy, New York: Routledge, 2020.

[23] T. Wheeler, „The First Electronic Network and the End of Time," în *From Gutenberg to Google: The History of Our Future,* Brookings Institution Press, 2019, p. 302.

[24] I. Popovici, „Criptografia, metoda pentru asigurarea securității tranzacțiilor de date," *Analele Științifice ale Universității de Stat „B. P. Hașdeu" din Cahul,* vol. VIII, 2012.

[25] C. Bartel, „The Puzzle of Historical Criticism.," *The Journal of Aesthetics and Art Criticism,* vol. 70, nr. 2, 2012.

[26] „Legal.up.ro," LegalUP, [Interactiv]. Available: https://legalup.ro/regulament-gdpr/. [Accesat 27 12 2023].

[27] „European Data Protection Board," [Interactiv]. Available: https://edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en. [Accesat 27 12 2023].

[28] M. Rosenberg, N. Confessore și C. Cadwalladr, „How Trump Consultants Exploited the Facebook Data of Millions," The New York Times, 17 3 2018. [Interactiv]. Available: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. [Accesat 27 12 2023].

[29] I. Barbu, Securitatea cibernetică: vulnerabilitățile sistemelor informatice ale viitorului, București: Școala Doctorală ETTI-B, Universitatea Politehnica din București, 2020.

[30] „Microsoft," 9 2019. [Interactiv]. Available: https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf. [Accesat 23 1 2024].

[31] Marsh & Microsoft, 9 2019. [Interactiv]. Available: https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf. [Accesat 27 12 2023].

[32] Workable Technology Limited, [Interactiv]. Available: https://resources.workable.com/cyber-security-policy. [Accesat 21 1 2024].

[33] R. Buchan, „Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?," *Journal of Conflict and Security Law,* vol. 17, nr. 2, 2012.

[34] NIST Computer Security Resource Center, [Interactiv]. Available: https://csrc.nist.gov/glossary/term/cyber_attack. [Accesat 29 12 2023].

[35] W. Motsch, A. David, K. Sivalingam și A. Wagner, „Approach for Dynamic Price-Based Demand Side Management in Cyber-Physical Production Systems," *Procedia Manufacturing,* vol. 51, pp. 1748-1754, 2020.

[36] M. Robinson, K. Jones și H. Janicke, „Cyber warfare: Issues and challenges," *Computers & Security,* vol. 49, pp. 70-94, 2015.

[37] Y. Li și Q. Liu, „A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Elsevier Ltd,* 2021.

[38] AAG, [Interactiv]. Available: https://aag-it.com/the-latest-cyber-crime-statistics/. [Accesat 29 12 2023].

[39] Arctic Wolf Solutions, 16 11 2022. [Interactiv]. Available: https://arcticwolf.com/resources/blog/decade-of-cybercrime/. [Accesat 29 12 2023].

[40] S. Morgan, „Cybercrime To Cost The World $10.5 Trillion Annually By 2025," [Interactiv]. Available: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/. [Accesat 29 12 2023].

[41] G. Santayana și J. Gouinlock, The Life of Reason or The Phases of Human Progress: Introduction and Reason in Common Sense, MIT Press, 2011.

[42] 31 5 2018. [Interactiv]. Available: https://www.schneier.com/blog/archives/2018/05/1834_the_first_.html. [Accesat 29 12 2023].

[43] „Cybersecurity history: hacking & data breaches," [Interactiv]. Available: https://www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches. [Accesat 29 12 2023].

[44] 2 11 2018. [Interactiv]. Available: https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218. [Accesat 29 12 2023].

[45] V. Popescu, „Vulnerabilități și amenințări din spațiul cibernetic vs. arhitectura de securitate la diferite niveluri," în *Conferința științifică internațională gândirea militară românească*, 2013.

[46] M. Dumitrascu, Dendrio, 2022. [Interactiv]. Available: https://www.dendrio.com/en/blog/7-metode-de-infectie-cu-ransomware/. [Accesat 29 12 2023].

[47] B. Smith, „Defending Ukraine: Early Lessons From the Cyber War," Microsoft, 6 2022. [Interactiv]. Available: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/. [Accesat 6 1 2024].

[48] C. Laurens, „Big Tech Cries Foul Over EU Cloud-Security Label," POLITICO, 14 6 2022. [Interactiv]. Available: https://www.politico.eu/article/tech-sector-foul-eu-cloud-security-label/. [Accesat 6 1 2024].

[49] „Cyber Resilience Act," European Commission, 9 2022. [Interactiv]. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act. [Accesat 6 1 2024].

[50] Verizon, [Interactiv]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[51] The White House, 13 5 2021. [Interactiv]. Available: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/. [Accesat 6 1 2024].

[52] Z. Whittaker, TechCrunch, 26 6 2019. [Interactiv]. Available: https://techcrunch.com/2019/07/26/marcus-hutchins-sentenced-kronos/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuYWNyb25pcy5jb20v&guce_referrer_sig=AQAAABWkQEnSkNqI14VtvNgmWH4iVh_tCTCy9cpGKYw2KD-Oz2bhlzHTitAt1FdnLkvx3dvL0plTIxhMPh2qOWpNl9k8irdB-tIa0SDkp3o4C. [Accesat 6 1 2024].

[53] Acronis Cyber Protect, [Interactiv]. Available: https://www.acronis.com/en-us/blog/posts/nhs-cyber-attack/. [Accesat 6 1 2024].

[54] G. Diamond, WestSideStory, 1 10 2021. [Interactiv]. Available: https://wsswired.com/4837/entertainment-3/the-2011-playstation-network-hack-what-actually-happened/. [Accesat 6 1 2024].

[55] European Commision, 15 9 2022. [Interactiv]. Available: https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act. [Accesat 6 1 2024].