DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

GHID DE IGIENĂ CIBERNETICĂ

pentru autoritățile și instituțiile publice locale din România

AUGUST 2025

TLP:CLEAR

CUPRINS

1. CONTEXT ȘI OBIECTIVE 3

2. AMENINȚĂRI SPECIFICE SECTORULUI PUBLIC LOCAL 3

2.1. Phishing și atacuri prin comunicații electronice 4
2.2. Ransomware și infrastructura atacurilor malware specializate 5
2.3. Compromiterea sistemelor de autentificare și control al accesului 6
2.4. Ingineria socială și manipularea factorului uman 7
2.5. Atacuri pe rețele Wi-Fi publice și interne 8
2.6. Compromiterea dispozitivelor USB și a altor medii portabile 9
2.7. Atacuri asupra aplicațiilor web ale instituției 10
2.8. Furtul de identitate digitală și fraude online 11
2.9. Atacuri asupra serviciilor cloud (Google Drive, OneDrive) 12
2.10. Atacuri asupra sistemelor locale Windows și a rețelei interne .. 13
2.11. Amenințări emergente 14

3. MĂSURI DE PROTECȚIE 15

3.1. Principii generale de securitate 15
3.2. Măsuri pentru protecția conturilor și autentificării 16
3.3. Protecția echipamentelor și rețelei interne 17
3.4. Securitatea serviciilor cloud 18
3.5. Securitatea aplicațiilor web 19
3.6. Protecția împotriva ransomware și malware 20
3.7. Conștientizarea și instruirea personalului 21
3.8. Managementul dispozitivelor portabile și mobile 22
3.9. Măsuri pentru amenințările emergente 23
3.10. Răspuns la incidente și planuri de continuitate 24

4. ASPECTE LEGALE ȘI de CONFORMITATE 25

4.1. Fluxuri de raportare către autoritățile competente 25
4.2. Responsabilități și bune practici de conformitate 25

5. PROCEDURI DE MANAGEMENT AL INCIDENTELOR CIBERNETICE 26

5.1. Clasificarea și prioritizarea incidentelor 26

6. IMPLEMENTARE ȘI MONITORIZARE 27

6.1. Etapele de implementare a măsurilor propuse 27
6.2. Verificarea măsurilor implementate 28
6.3. Roluri și responsabilități 28
6.4. Plan de pregătire continuă și revizuire anuală 29

7. CONCLUZII ȘI RECOMANDĂRI STRATEGICE 30

ANEXA 1 - Checklist de securitate cibernetică 31

ANEXA 2 - Proceduri pas-cu-pas pentru situații de criză 32

ANEXA 3 - Lista de contacte utile 33

ANEXA 4 - Studiu de caz - Primăria Sector 5 București 34

ANEXA 5 - Glosar de termeni și acronime 35

NOTE DE FINAL 38

1. CONTEXT ȘI OBIECTIVE

Administrația publică locală din România se află într-un proces accelerat de digitalizare, cu scopul de a eficientiza serviciile publice și de a crește transparența. Deși această evoluție este benefică, ea expune instituțiile la riscuri cibernetice tot mai mari, într-un mediu digital complex și greu de controlat. Multe autorități locale funcționează cu infrastructuri informatice învechite, resurse financiare limitate pentru securitatea IT și personal insuficient specializat. În lipsa unor măsuri clare și constante de protecție, aceste vulnerabilități pot fi exploatate cu ușurință de atacatori. Un incident cibernetic poate avea consecințe imediate, cum ar fi întreruperea serviciilor publice, pierderea datelor sensibile, afectarea reputației instituției sau aplicarea de sancțiuni legale. Securitatea cibernetică nu mai este o opțiune, ci o condiție esențială pentru funcționarea stabilă, sigură și credibilă a administrației locale. De aceea, instituțiile trebuie să adopte o abordare proactivă, care să combine măsuri de protecție tehnice, reguli interne clare, instruire continuă și mecanisme eficiente de răspuns la incidente.

În acest context, prezentul ghid este conceput pentru a sprijini autoritățile publice locale în procesul de consolidare a igienei cibernetice, prin recomandări practice și adaptate contextului operațional. Prin acest document, ne propunem să oferim o imagine clară a principalelor amenințări informatice și să propunem măsuri concrete de prevenire, detecție și reacție. Aceste măsuri sunt în concordanță cu reglementările în vigoare, cum ar fi OUG nr. 155/2024 și Regulamentul general privind protecția datelor (GDPR). Am abordat teme esențiale precum atacurile de tip phishing, ransomware, compromiterea conturilor, securitatea serviciilor cloud și a aplicațiilor web, riscurile Bring Your Own Device (BYOD) și amenințările emergente precum deepfake și atacurile asistate de inteligență artificială (IA). Ghidul include, de asemenea, proceduri de gestionare a incidentelor, bune practici, instrumente de autoevaluare lunară și un glosar explicativ al termenilor specifici.

Prin aplicarea acestor măsuri, instituțiile publice locale pot reduce semnificativ expunerea la riscuri, pot proteja datele cetățenilor și pot menține continuitatea serviciilor esențiale, consolidând, în același timp încrederea publică și reziliența organizațională.

2. AMENINȚĂRI SPECIFICE SECTORULUI PUBLIC LOCAL

Acest capitol descrie principalele tipuri de amenințări cibernetice cu care se confruntă instituțiile publice locale din România (primării, consilii județene etc.). Sunt evidențiate, într-o manieră structurată și accesibilă, caracteristicile tehnice ale acestor vulnerabilități, modul în care sunt exploatate de atacatori și motivele pentru care aceste entități sunt ținte atractive și profitabile.[1]

Fiecare subsecțiune prezintă impactul potențial asupra funcționării instituției și asupra protecției datelor cetățenilor. De asemenea, sunt incluse exemple concrete, adaptate realității administrației publice locale. Informațiile cuprinse în acest capitol constituie fundamentul necesar pentru înțelegerea riscurilor specifice mediului digital instituțional. Măsurile concrete de prevenire, detecție și protecție vor fi detaliate în capitolele următoare.

2.1. Phishing și atacuri prin comunicații electronice

***Phishing-ul** reprezintă o tentativă frauduloasă de a obține informații sensibile, cum ar fi date de conectare, informații despre cardul bancar sau situația financiară, folosind ingineria socială. Atacatorii se deghizează ca reprezentanți ai unor entități de încredere (ex: bănci, companii, instituții publice) cel mai adesea prin e-mail, mesaje text (smishing) sau apeluri telefonice (vishing), pentru a convinge victimele să efectueze o anumită acțiune.*[2]

În mediul administrației publice locale, phishing-ul are o eficiență ridicată datorită specificului activităților birocratice, prin care funcționarii primesc frecvent cereri urgente de la instituții superioare și se confruntă cu termene stricte și cu riscul de sancțiuni. Atacatorii exploatează aceste caracteristici pentru a induce în eroare angajații, determinându-i să divulge informații sensibile sau să realizeze acțiuni care compromit securitatea instituție.

Printre tipologiile de phishing posibile se numără:

- **spear phishing**: reprezintă atacuri de tip phishing personalizate și direcționate către un anumit individ sau o categorie specifică de angajați, folosind informații despre persoana vizată pentru a crește credibilitatea mesajului. Atacatorii pot analiza poziția profesională a victimei, relațiile instituționale sau comunicările publice pentru a crea mesaje aparent legitime. Spear phishing-ul presupune un nivel ridicat de pregătire și adaptare la contextul victimei;
- **whaling**: reprezintă atacuri de tip phishing, direcționate special către persoane cu funcții de conducere, precum primari sau directori, având ca scop obținerea de informații sensibile sau determinarea acestora să inițieze acțiuni cu impact dăunător care pot compromite securitatea informațiilor sau integritatea instituției;
- **Business Email Compromise (BEC)**: atacuri în care infractorii cibernetici se prezintă drept superiori ierarhici, colegi sau parteneri instituționali, cu scopul de a obține transferuri de date, efectuarea de plăți sau alte acțiuni care să le aducă beneficii;
- **deepfake voice phishing**: utilizarea tehnologiilor bazate pe IA pentru a imita vocea unor oficiali, crescând credibilitatea mesajelor transmise.

Consecințele unui atac de tip phishing pot fi diverse, de la accesul neautorizat la baze de date cu informații personale, până la modificarea sau ștergerea documentelor oficiale, interceptarea comunicațiilor interne sau compromiterea comunicărilor oficiale în context electoral. În plus, compromiterea unui singur cont poate facilita atacuri ulterioare la nivelul altor instituții publice, având potențialul de a afecta inclusiv niveluri județene, regionale sau naționale. Incidentele de acest tip pot cauza întârzieri semnificative în furnizarea serviciilor publice și pot eroda încrederea cetățenilor în capacitatea administrației publice locale de a proteja datele personale și de a asigura continuitatea serviciilor esențiale.

Figură 1. Exemplu de phishing

Exemplu: o secretară din cadrul unei primării primește un SMS care pare trimis de la Ministerul Dezvoltării, solicitând actualizarea urgentă a datelor pentru un proiect cu finanțare europeană, prin accesarea unui link. Mesajul reproduce elemente vizuale și un ton birocratic specific comunicărilor oficiale. Prin introducerea datelor de autentificare pe site-ul fals, atacatorul ar putea obține acces neautorizat la sistemele informatice ale instituției.

2.2. Ransomware și infrastructura atacurilor malware specializate

***Ransomware** reprezintă un tip de software dăunător (malware) care fie criptează fișierele sau întregul sistem al victimei, acestea devenind inaccesibile, fie blochează accesul la dispozitiv și cere ulterior o plată (răscumpărare), adesea în criptomonede, pentru a restabili accesul sau pentru a preveni publicarea/ștergerea datelor.*

Un incident ransomware poate paraliza complet activitatea unei instituții din administrația publică locală, blocând accesul angajaților la fișiere și aplicații esențiale. Statisticile arată că 34% dintre organizațiile guvernamentale locale au fost afectate de ransomware în 2024, iar costul mediu de recuperare a fost de 2,83 milioane de dolari.[3,4]

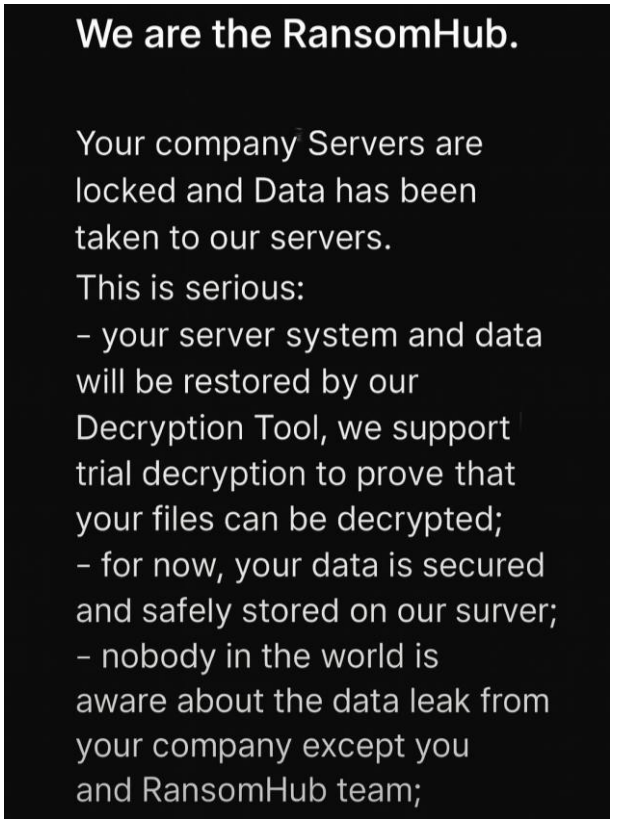
Atacurile de tip ransomware au evoluat semnificativ în ultimii ani, existând forme din ce în ce mai sofisticate, precum:

- **ransomware multi-stage**: atacuri complexe care includ faze preliminare de spionaj și recunoaștere în infrastructura victimei;
- **living-off-the-land attacks**: utilizarea unor instrumente legitime ale sistemului de operare sau ale rețelei pentru desfășurarea acțiunilor dăunătoare, îngreunând astfel detecția;
- **supply chain malware**: infectarea software-ului prin actualizări legitime sau prin compromiterea furnizorilor de servicii;
- **wiperware**: malware care șterge definitiv datele, fără solicitare de răscumpărare.

Vectorii de intruziune în astfel de atacuri includ expunerea necontrolată a serviciilor de acces la distanță Remote Desktop Protocol (RDP), exploatarea vulnerabilităților în soluții de tip rețea virtuală privată (Virtual Private Network/VPN) sau utilizarea documentelor cu comenzi macro malițioase.

O problemă majoră este lipsa mecanismelor eficiente de recuperare. Backup-urile pot fi inexistente, compromise sau învechite, ceea ce duce la pierderi semnificative de date. Astfel, o primărie poate pierde luni sau chiar ani de documente și evidențe digitale, ceea ce generează costuri considerabile pentru restabilirea informațiilor. În sectorul public, apare și dilema juridică și etică legată de plata unei răscumpărări. Utilizarea fondurilor publice pentru o astfel de plată poate încălca reglementările și poate crea un precedent periculos. Pe de altă parte, refuzul plății poate prelungi blocajele instituționale și afecta serviciile publice.

Un concept recent utilizat de grupările de ransomware este double extortion, caz în care, pe lângă criptarea datelor, atacatorii amenință că vor publica informațiile sustrase. În cazul administrației publice, publicarea dosarelor personale, a corespondenței interne sau a documentelor sensibile poate genera crize de imagine, anchete jurnalistice și consecințe politice.



Figură 2. Mesaj al hackerilor care au atacat serverele Primăriei Sectorului 5

Exemplu: în urma unui e-mail aparent trimis de la Direcția Generală Economică, un angajat din cadrul unei primării a descărcat un fișier Excel care părea a conține un model de raportare bugetară. Fișierul conținea un macro malițios care, odată activat, a declanșat criptarea documentelor de pe stația de lucru și, ulterior, propagarea în rețeaua internă. Instituția nu avea un sistem de backup funcțional, iar datele financiare ale ultimilor 3 ani au fost inaccesibile timp de două săptămâni. Atacatorii au cerut o răscumpărare de 3 BTC.

2.3. Compromiterea sistemelor de autentificare și control al accesului

Compromiterea sistemelor de autentificare și control al accesului *reprezintă obținerea neautorizată a credențialelor sau exploatarea mecanismelor de validare (parole, token-uri, factori multipli) pentru accesul fraudulos în rețelele și aplicațiile instituției.*

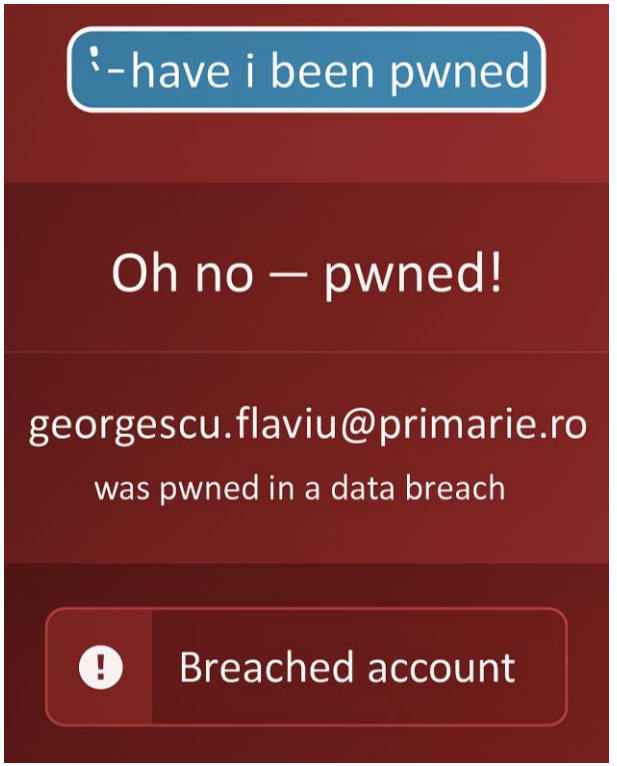
În multe instituții publice locale, o problemă majoră este utilizarea parolelor simple și ușor de ghicit, cum ar fi „Primaria123”, „parola” sau combinații care includ numele instituției. Această practică se datorează, de regulă, lipsei de conștientizare a importanței unor parole complexe și existenței unor sisteme informatice învechite, care nu permit aplicarea unor politici stricte de gestionare a parolelor. O situație frecventă este reutilizarea acelorași parole pentru mai multe sisteme, inclusiv pentru accesul la e-mail-uri personale, rețele sociale sau aplicații de gestionare a resurselor instituției. Astfel, un atacator care obține o parolă dintr-o scurgere de date online are șanse mari să pătrundă în infrastructura informatică a instituției publice.[5]

Atacurile asupra credențialelor includ, printre altele:

- **password spraying**: tehnică de atac prin care o parolă simplă sau un set redus de parole frecvente (de exemplu, „Parola123”, „Admin2025”) este testat pe un număr mare de conturi. Scopul acestei metode este de a evita blocarea conturilor, spre deosebire de atacurile brute-force clasice, care implică numeroase încercări repetate asupra unui singur cont. Această tehnică este eficientă în medii în care parolele sunt simple și previzibile, iar mecanismele de protecție (precum autentificarea multi-factor, blocarea temporară după încercări eșuate sau limitarea numărului de autentificări) lipsesc sau nu sunt aplicate corect;
- **credential stuffing**: exploatarea reutilizării acelorași parole pe conturi diferite. Atacatorii folosesc baze de date cu credențiale furate din breșe anterioare (email + parolă) și le testează automat pe alte platforme, în speranța că utilizatorii au folosit aceeași combinație;
- **token hijacking**: furtul sau capturarea token-urilor de autentificare utilizate în sistemele de tip Single Sign-On (SSO) – mecanisme care permit accesul la mai multe aplicații printr-o singură autentificare. Token-ul acționează ca o „cheie temporară” ce dovedește că utilizatorul s-a autentificat deja, fără a mai introduce parola de fiecare dată.

Vulnerabilitățile asociate autentificării multi-factor pot include interceptarea codurilor prin SMS (ex. SIM swapping), compromiterea aplicațiilor de autentificare prin malware mobil, utilizarea ingineriei sociale pentru ocolirea celui de-al doilea factor și accesul la codurile de rezervă stocate nesecurizat.

O altă problemă majoră întâlnită în administrația publică este incompatibilitatea sistemelor informatice vechi cu soluțiile moderne de autentificare. Actualizarea acestor sisteme presupune costuri ridicate și perioade de întrerupere a activității, aspecte dificil de gestionat pentru multe instituții publice. Astfel, persistă o vulnerabilitate semnificativă în ceea ce privește controlul accesului și securitatea generală a infrastructurii informatice.



Figură 3. Exemplu de adresă instituțională compromisă într-o breșă de date, verificabilă prin platforma haveibeenpwned.com

Exemplu: dacă parolele unui utilizator au fost compromise într-o breșă la Facebook (ex. ana.123@yahoo.com / parola123), atacatorii le pot testa pe Gmail, contul instituțional sau alte servicii online. Dacă parola este reutilizată, atacul va avea succes fără efort suplimentar.

2.4. Ingineria socială și manipularea factorului uman

Ingineria socială și manipularea factorului uman *reprezintă ansamblul de tehnici de persuasiune și influențare psihologică prin care atacatorii induc utilizatorii în eroare, determinându-i să divulge informații sensibile sau să întreprindă acțiuni neautorizate care compromit securitatea sistemelor și datelor instituției.*[6]

Atunci când tehnologia nu permite accesul direct, atacatorii apelează la tehnici de inginerie socială pentru a manipula factorul uman și a obține informații sensibile sau acces neautorizat la resursele informatice ale instituțiilor publice. În mediul administrației publice locale, ingineria socială exploatează caracteristici specifice acestui domeniu, precum respectul pentru ierarhie, presiunea termenelor administrative, colaborarea interinstituțională și teama de sancțiuni. Prin exploatarea acestor particularități, atacatorii își sporesc șansele de reușită în obținerea de informații sau în declanșarea unor acțiuni care compromit securitatea instituțională.

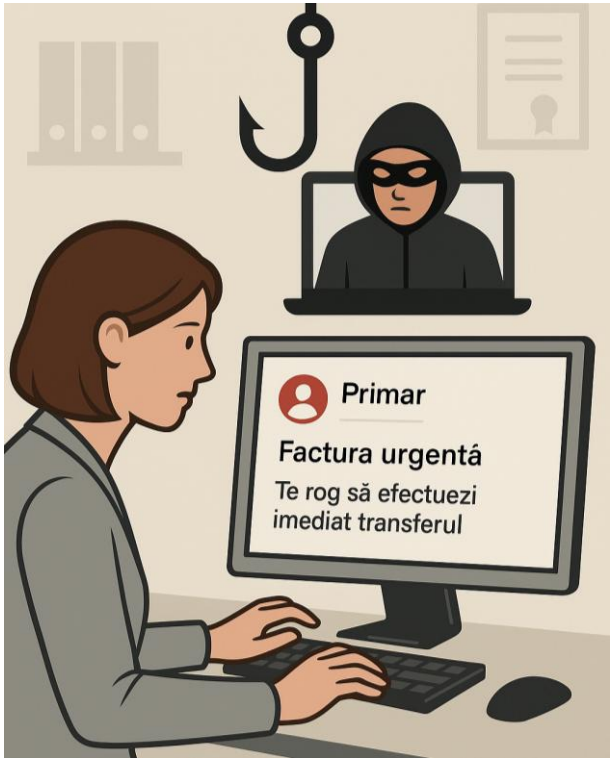
Tehnicile frecvent utilizate în atacurile de inginerie socială includ:

- **pretexting**: crearea unor scenarii administrative credibile, prin care atacatorul se prezintă ca reprezentant al unei instituții superioare sau ca persoană cu atribuții oficiale;
- **baiting**: oferirea de beneficii, premii sau informații exclusive, pentru a stimula curiozitatea sau interesul angajaților;
- **quid pro quo**: exploatarea culturii schimbului de favoruri, prin promisiunea efectuării unui serviciu sau obținerii unor avantaje în schimbul unor informații confidențiale;
- **tailgating**: intrarea neautorizată în spații fizice sau digitale, prin urmărirea persoanelor autorizate sau prin folosirea de legitimații și pretexte false.

Perioada pandemică și cea post-pandemică a reprezentat un context favorabil pentru astfel de atacuri. Amenințările au fost mascate sub forma unor măsuri de sănătate publică, a unor proceduri administrative legate de lucrul hibrid sau a ofertelor de soluții tehnologice „gratuite”, menite să faciliteze activitatea instituțiilor. Scenariile administrative credibile reprezintă principala armă a atacatorilor. Aceștia studiază atent structura organizațională, procedurile uzuale, calendarul activităților politice și administrative, precum și alte informații relevante.

Cunoașterea termenelor legate de proiectele finanțate din fonduri europene, a perioadelor de raportare către autoritățile județene sau a calendarului electoral le permite atacatorilor să identifice momente de maximă presiune, transformând aceste perioade în oportunități pentru lansarea atacurilor.

În prezent, atacurile asistate de IA sunt pe un trend ascendent, tehnologia este folosită pentru a personaliza atacurile la scară largă, analizând comunicările publice ale oficialilor (declarații, postări, înregistrări audio) și stilul documentelor oficiale. Pe baza acestor date, IA generează automat mesaje care reproduc fidel limbajul și tonul persoanelor vizate, sporind credibilitatea atacurilor.



Figură 4. E-mail de tip phishing care imită o cerere oficială din partea conducerii

Exemplu: o angajată din departamentul financiar primește un e-mail care pare trimis de primar, cerând plata urgentă a unei facturi. Mesajul conține numele real al furnizorului și semnătura digitală copiată din corespondențe anterioare. Fără să verifice telefonic solicitarea sau adresa expeditorului, angajata efectuează plata către un cont indicat în e-mail, care aparținea, de fapt, atacatorilor.

2.5. Atacuri pe rețele Wi-Fi publice și interne

Atacurile asupra rețelelor Wi-Fi publice și interne *reprezintă acțiuni malițioase prin care atacatorii exploatează vulnerabilitățile configurațiilor rețelelor fără fir (wireless) pentru a intercepta comunicațiile, a obține acces neautorizat la resursele instituției și a lansa atacuri ulterioare asupra infrastructurii informatice.*

Majoritatea instituțiilor publice locale oferă conexiuni Wi-Fi pentru angajați și/sau vizitatori. Deși aceste servicii facilitează activitatea zilnică și accesul cetățenilor la resurse, ele pot constitui un punct vulnerabil major dacă nu sunt configurate și securizate corespunzător. Riscurile asociate nu se limitează doar la accesul gratuit la Internet în proximitatea instituției, ci includ și posibilitatea ca atacatorii să utilizeze aceste conexiuni drept punct de lansare a unor atacuri asupra rețelei interne.

Printre atacurile frecvent întâlnite se numără:

- **puncte de acces false (evil twin):** reprezintă rețele Wi-Fi malițioase create în proximitatea instituției, care preiau denumirea și setările rețelei oficiale, cu scopul de a-i determina pe utilizatori să se conecteze și de a le intercepta sau manipula datele transmise;
- **atacuri de de-autentificare (Deauthentication Attacks)**: atacatorul forțează deconectarea dispozitivelor utilizatorilor de la rețelele Wi-Fi legitime, cu scopul de a le redirecționa către rețele controlate (rogue AP) sau pentru a intercepta pachetele de autentificare transmise în momentul reconectării (ex. capturarea „handshake-ului” WPA2, utilizat ulterior în atacuri de tip offline password cracking);
- **exploatarea vulnerabilităților în protocoalele WPA2/WPA3**: vulnerabilități existente în rețelele mai vechi, care permit interceptarea traficului sau accesul neautorizat;
- **falsificarea paginilor captive**: crearea unor pagini false de autentificare, care solicită utilizatorilor introducerea credențialelor de acces. Utilizatorii sunt încurajați să-și introducă datele de conectare, care sunt apoi interceptate de atacatori.

O problemă majoră în rețelele instituțiilor publice o constituie segmentarea inadecvată a infrastructurii. În multe cazuri, rețeaua destinată vizitatorilor nu este separată corespunzător de cea administrativă, ceea ce poate expune resursele instituției la atacuri cibernetice. Un atacator care obține acces la rețeaua publică poate identifica și ataca dispozitivele angajaților, similar cu situația în care cheia este lăsată în yală la o poartă între curtea publică și biroul primarului.

Politicile de tip BYOD pot genera riscuri suplimentare pentru securitatea cibernetică, deoarece implică utilizarea, de către angajați, a dispozitivelor personale, precum telefoane sau laptopuri, conectate la rețeaua instituției. Aceste dispozitive pot fi vulnerabile sau chiar infectate cu malware, ceea ce poate facilita răspândirea codului malițios în infrastructura critică a instituției și crește riscul compromiterii sistemelor informatice.

Figură 5. Imagine simbolică a unei victime care se conectează la o rețea Wi-Fi falsă, fără să știe că atacatorii interceptează toate datele transmise

Exemplu: un angajat al primăriei se conectează la o rețea Wi-Fi cu nume identic cu cel al rețelei instituției. Fără să știe că este falsă, introduce datele de autentificare, care ajung direct la atacatori. Aceștia pot folosi datele de acces pentru a compromite sistemele interne ale instituției.

2.6. Compromiterea dispozitivelor USB și a altor medii portabile

Compromiterea dispozitivelor USB și a altor medii portabile *reprezintă procesul prin care dispozitivele de stocare detașabile (stick-uri USB, CD-uri, DVD-uri, carduri de memorie etc.) sunt infectate sau manipulate pentru a introduce software malițios în rețeaua instituției ori pentru a exfiltra date sensibile fără detectare.*

Dispozitivele USB continuă să fie utilizate pe scară largă în administrația publică locală pentru transferul de date între instituții care nu dispun de sisteme integrate, pentru realizarea de copii de siguranță pe suporturi portabile sau pentru prezentări în cadrul ședințelor. Această dependență generează o suprafață extinsă de atac, exploatabilă de către infractorii cibernetici. Conform raportului Honeywell[7] din anul 2024, 51% din atacurile malware sunt concepute pentru dispozitive USB, o creștere de șase ori comparativ cu anul 2019.

Tipuri frecvente de atacuri prin medii portabile includ:

- **USB cu firmware modificat**: dispozitive care imită funcționalitatea unui stick de memorie, dar care sunt programate să se identifice ca tastaturi și să execute automat comenzi, fără intervenția utilizatorului;
- **stick-uri USB cu script-uri autorun**: conțin script-uri care se activează imediat după conectare și pot iniția acțiuni malițioase pe echipamentele victimei;
- **malware persistent**: programe malițioase care rămân active pe dispozitive, chiar dacă acestea par curate sau au fost supuse unor procese de dezinfectare;
- **dispozitive de exfiltrare**: stick-uri sau alte suporturi mobile care, deși par inofensive, sunt concepute să copieze automat datele la care au acces.

Pe lângă dispozitivele USB, există și alte medii portabile care pot fi compromise, precum CD-uri sau DVD-uri ce conțin software, prezentări sau formulare aparent legitime sau carduri de memorie „uitate” în spațiile publice ale instituției. De asemenea, transferurile de date realizate prin aplicații de mesagerie pe dispozitive mobile pot reprezenta surse de risc, mai ales dacă sunt utilizate în mod necontrolat pentru schimbul de documente de serviciu.

Un vector important de succes al acestor atacuri rămâne curiozitatea umană. Este frecventă tehnica prin care atacatorii lasă stick-uri USB infectate în locuri vizibile, cum ar fi parcările instituțiilor publice, etichetate sugestiv cu titluri precum „Salarizare 2025”, „Proiect fonduri UE” sau „Fotografii eveniment”. Angajații care găsesc astfel de dispozitive și le conectează la computerele instituției pot declanșa, involuntar, compromiterea rețelei interne.

În administrația publică locală, atacurile prin medii portabile sunt eficace deoarece multe instituții depind, încă, de transferul fizic de date. Practici precum utilizarea de CD-uri de la instituții centrale, stick-uri USB cu formulare sau backup-uri pe suporturi externe sunt frecvente. În multe cazuri, aceste dispozitive nu beneficiază de un control adecvat, din cauza resurselor financiare limitate, a dependenței de metode tradiționale sau a insuficientei expertize tehnice.

Figură 6. Utilizarea mediilor portabile nesigure expune rețeaua instituției la riscuri majore

Exemplu: un angajat găsește în parcare un stick USB etichetat „Proiect fonduri UE” și îl conectează la calculatorul instituției, din curiozitate. Dispozitivul, aparent inofensiv, conține un script care rulează automat și instalează un malware ce permite atacatorilor acces de la distanță la rețeaua internă a instituției.

2.7. Atacuri asupra aplicațiilor web ale instituției

***Atacurile asupra aplicațiilor** web constau în exploatarea vulnerabilităților existente în codul sursă, în configurările aplicației sau în mecanismele de autentificare ale interfețelor web publice ale instituției. Scopul acestor atacuri poate fi obținerea accesului neautorizat la date, compromiterea confidențialității și integrității informațiilor sau întreruperea funcționării normale a serviciilor digitale.*

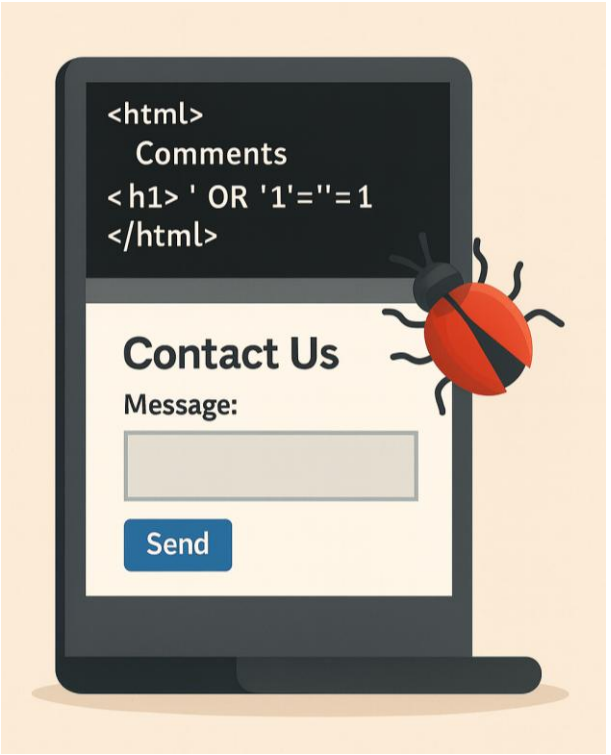
Site-ul oficial al primăriei reprezintă, de cele mai multe ori, prima și cea mai vizibilă țintă pentru atacatorii cibernetici, fiind perceput ca o „vitrină vulnerabilă" a instituției[8]. Interesul infractorilor nu se limitează la acțiuni de vandalism digital, precum înlocuirea mesajelor de pe prima pagină, ci vizează și accesarea sistemelor aflate în spatele interfeței publice, inclusiv a bazelor de date cu informații despre cetățeni, a sistemelor de management al documentelor sau a aplicațiilor destinate activităților administrative, precum cele de urbanism.

Aplicațiile web ale instituțiilor publice pot prezenta vulnerabilități care pot fi exploatate prin:

- **injecții SQL**: exploatarea formularelor de contact sau a funcțiilor de căutare de pe site pentru a executa comenzi neautorizate în bazele de date;
- **Cross-Site Scripting (XSS)**: reprezintă o formă de atac informatic care presupune injectarea de cod malițios (cel mai frecvent JavaScript) în componente ale unei aplicații web, precum câmpuri de comentarii, formulare sau secțiuni de anunțuri publice. Scopul acestor atacuri este compromiterea dispozitivelor utilizatorilor care accesează respectivele pagini. Prin exploatarea unei astfel de vulnerabilități, atacatorii pot redirecționa utilizatorii către site-uri controlate, pot fura credențiale de autentificare sau session cookies, pot executa acțiuni în numele utilizatorilor autentificați (atacuri de tip session hijacking) ori pot colecta date sensibile fără consimțământul victimei;
- **Cross-Site Request Forgery (CSRF)**: lansarea de acțiuni malițioase în aplicațiile administrative interne, exploatând sesiunile autentificate ale utilizatorilor;
- **referințe directe nesecurizate**: accesul neautorizat la documente și fișiere sensibile prin manipularea link-urilor de acces direct către resursele publicate.

Administrația publică locală se confruntă cu provocarea integrării noilor aplicații web în infrastructuri informatice depășite, cu necesitatea respectării standardelor de accesibilitate și a compatibilității cu browsere învechite, toate sub presiunea lansării rapide a serviciilor digitale. Această presiune pentru digitalizare accelerată a determinat dezvoltarea rapidă a numeroase aplicații web, precum platforme pentru plata taxelor și impozitelor, cereri de eliberare a certificatelor sau programări online.

În multe cazuri, aceste soluții au fost realizate de firme mici, cu experiență limitată în domeniul securității cibernetice, în timp foarte scurt și cu bugete restrânse, ceea ce poate reprezenta un potențial risc în ceea ce privește asigurarea unui nivel adecvat de securitate.



Figură 7. Atac prin formular web nesecurizat, punct de intrare pentru cod malițios

Exemplu: formularele de contact publicate pe site-urile instituțiilor pot reprezenta un vector de atac, dacă nu sunt securizate corespunzător. Codul malițios introdus de atacator poate fi executat automat atunci când mesajul este deschis de un angajat, ceea ce poate duce la compromiterea dispozitivului și, ulterior, a întregii rețele informatice.

2.8. Furtul de identitate digitală și fraude online

Furtul de identitate digitală *reprezintă sustragerea și utilizarea neautorizată a datelor personale sau a credențialelor unui utilizator în mediul online, în scopul comiterii de fraude, obținerii de avantaje necuvenite sau accesului neautorizat la sistemele și resursele informaționale ale instituției.*

Funcționarii publici locali constituie ținte atractive pentru atacurile cibernetice care urmăresc furtul de identitate digitală. Aceștia dețin acces la informații sensibile despre cetățeni, pot influența decizii administrative și beneficiază de un nivel ridicat de încredere în cadrul comunității.

Un atacator care reușește să își însușească identitatea unui funcționar public poate obține câștiguri financiare nelegitime sau poate manipula procese administrative în interes propriu.

Mecanisme frecvent utilizate în compromiterea identității digitale:

- **preluarea conturilor**: exploatarea reutilizării parolelor între conturile personale și cele profesionale ale funcționarilor;
- **crearea de identități sintetice**: construirea unor identități fictive, bazate pe combinații între date reale ale funcționarilor și informații false;
- **imitarea oficialilor prin tehnologia deepfake**: utilizarea tehnologiilor audio sau video pentru a reproduce vocea, înfățișarea sau comportamentul unor persoane reale, cu scopul de a manipula deciziile administrative;
- **colectarea de date din rețelele sociale**: utilizarea informațiilor publicate de funcționari pe platformele sociale pentru elaborarea unor atacuri de inginerie socială mai credibile.

Implicațiile furtului de identitate în administrația publică locală pot fi multiple și grave și pot include:

- manipularea proceselor de urbanism;
- influențarea procedurilor de licitație publică;
- accesarea neautorizată a dosarelor cetățenilor;
- scurgerea de informații confidențiale către mass-media sau către competitori politici.

Un element important în aceste atacuri îl reprezintă profilarea prin rețelele sociale, care constituie adesea primul pas al infractorilor cibernetici. Mulți funcționari publici dețin conturi active pe rețelele sociale, unde publică informații despre activitatea profesională, participarea la evenimente oficiale sau fotografii din birou. Aceste informații permit atacatorilor să construiască profiluri detaliate ale funcționarilor, identificând cine sunt, cum comunică și ce responsabilități dețin, precum și aspecte legate de perioadele de concediu.

Figură 8. Furtul de identitate digitală prin analiza profilurilor online ale funcționarilor

Exemplu: un scenariu plauzibil ar putea fi cel în care un atacator studiază profilul unui arhitect-șef din cadrul unei primării, după care contactează dezvoltatori imobiliari pretinzând că poate „grăbi" aprobarea certificatelor de urbanism în schimbul unor sume de bani. Utilizând informații reale despre dosare - obținute fie din surse publice, fie prin atacuri de tip phishing - atacatorul poate crea aparența că discută cu funcționarul real, determinând, astfel, dezvoltatorii să efectueze plăți substanțiale înainte ca frauda să fie descoperită.

2.9. Atacuri asupra serviciilor cloud (Google Drive, OneDrive)

Atacurile asupra serviciilor cloud *reprezintă acțiuni malițioase concepute pentru a compromite confidențialitatea, integritatea sau disponibilitatea datelor și aplicațiilor găzduite pe platforme cloud (de exemplu Google Drive, OneDrive), prin exploatarea configurărilor incorecte, a credențialelor compromise, a vulnerabilităților interfeței de programare a aplicației (API) sau a practicilor neautorizate de tip „shadow IT”.*

Serviciile cloud, precum Google Drive, OneDrive sau Dropbox, sunt utilizate regulat în administrația publică locală, datorită avantajelor pe care le oferă în ceea ce privește accesul rapid la date, colaborarea la distanță și eficiența operațională. Totuși, aceste soluții aduc cu ele o serie de riscuri specifice, adesea subestimate sau insuficient înțelese în mediul instituțiilor publice locale.

Riscuri asociate utilizării serviciilor cloud în administrația publică locală:

- **configurări incorecte ale permisiunilor de acces**: o eroare frecventă este acordarea de drepturi extinse asupra documentelor, făcându-le accesibile publicului larg sau persoanelor neautorizate;
- **shadow IT**: utilizarea, fără aprobare oficială, a serviciilor cloud personale pentru derularea activităților instituționale, ceea ce implică transferul de date oficiale pe platforme care nu sunt sub controlul administrației;
- **încălcarea reglementărilor privind stocarea datelor**: transferul sau stocarea datelor personale ale cetățenilor în afara Uniunii Europene (UE) poate contraveni cerințelor legale de protecție a datelor;
- **dependența excesivă de furnizor**: întreruperile serviciilor sau modificările de politică ale furnizorului pot afecta accesul instituției la date și la documente sensibile.

Serviciile cloud pot fi ținta unor atacuri cibernetice diverse, inclusiv compromiterea platformelor de e-mail, atacuri asupra sistemelor de partajare a fișierelor, infiltrarea în instrumentele de colaborare și extinderea atacurilor ransomware către backup-urile salvate în cloud.

În administrația publică locală, o problemă frecventă este Shadow IT, adică folosirea de către angajați a unor conturi personale (ex. Gmail, OneDrive) pentru activități oficiale, cum ar fi transmiterea de documente voluminoase, colaborarea la distanță sau partajarea de fișiere. În acest mod, datele instituției ajung pe platforme necontrolate, iar compromiterea unui cont personal poate duce la expunerea de documente sensibile.

GDPR impune cerințe stricte în utilizarea serviciilor cloud, în special a celor operate de companii din afara UE. Multe instituții publice locale nu conștientizează că stocarea datelor personale ale cetățenilor pe platforme precum Google Drive sau OneDrive poate încălca legislația privind protecția datelor, expunându-se, astfel, la sancțiuni care pot ajunge până la 4% din bugetul anual al instituției.

Figură 9. Acces neautorizat la servicii cloud - risc cibernetic major

Exemplu: un angajat al unei primării a folosit contul său personal de Google Drive pentru a partaja un document de lucru intern. Ulterior, contul său a fost compromis în urma unui atac de tip phishing, iar documentele încărcate, inclusiv liste cu date personale ale cetățenilor, au devenit accesibile atacatorului. Incidentul a generat o notificare către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) și a dus la suspendarea temporară a accesului la platformele cloud.

2.10. Atacuri asupra sistemelor locale Windows și a rețelei interne

Atacurile asupra sistemelor locale Windows și a rețelei interne *reprezintă exploatarea vulnerabilităților din sistemele de operare Windows (stații de lucru și servere) și din infrastructura internă de rețea, pentru a obține acces neautorizat, a escalada privilegii, a mișca lateral între resurse și a menține persistența în mediul instituțional.*

Aceste atacuri pot folosi tehnici precum:

- **escaladarea privilegiilor**: exploatarea vulnerabilităților locale neactualizate pentru a obține drepturi de administrator pe sisteme critice;
- **mișcarea laterală în rețea**: navigarea atacatorilor între diverse echipamente și servere, în special în medii Active Directory configurate incorect;
- **abuzul PowerShell**: utilizarea PowerShell pentru rularea de coduri malițioase, greu de detectat în activitatea normală a sistemelor;
- **atacuri prin Windows Management Instrumentation (WMI)**: tehnici utilizate pentru menținerea persistenței și ascunderea activității malițioase în infrastructura rețelei.

De asemenea, vulnerabilitățile existente în rețelele locale includ:

- **segmentarea insuficientă a rețelei**: situații în care stațiile de lucru au acces direct la servere critice, fără limitări corespunzătoare;
- **utilizarea protocoalelor depășite**: metode de comunicare învechite care nu mai oferă suficientă protecție, poate permite interceptarea traficului din rețea sau lansarea de atacuri de tip „om la mijloc” (*man-in-the-middle*), prin care atacatorii pot vedea sau modifica informațiile transmise);
- **atacuri DNS interne**: atacatorii pot compromite serverele interne DNS, care au rolul de a asocia numele site-urilor cu adresele IP corespunzătoare, redirecționând, astfel, traficul către servere controlate de ei. Acest tip de atac poate permite interceptarea datelor sau lansarea altor acțiuni malițioase în rețea;
- **saltul între VLAN-uri**: exploatarea unor configurări incorecte ale rețelei, care permit atacatorilor să treacă neautorizat dintr-un segment de rețea în altul (de exemplu, dintr-o zonă publică într-un VLAN administrativ), obținând astfel acces la resurse interne protejate.

O problemă fundamentală în administrația publică locală este managementul deficitar al actualizărilor de securitate (patch management). În multe instituții, actualizările de sistem sunt dezactivate de teamă că ar putea provoca disfuncționalități în aplicațiile zilnice. Procedurile birocratice, necesare pentru aprobarea oricărei modificări tehnice, și reticența la schimbare duc la întârzieri în aplicarea patch-urilor critice. Între timp, atacatorii monitorizează îndeaproape vulnerabilitățile cunoscute și le exploatează pentru a pătrunde în infrastructura informatică a instituțiilor.

Figură 10. Escaladare de privilegii prin exploatarea unui document malițios

Exemplu: Un scenariu frecvent întâlnit presupune escaladarea privilegiilor prin exploatarea unor vulnerabilități neactualizate. De exemplu, un angajat poate deschide un document aparent legitim, care conține cod malițios. Malware-ul exploatează o vulnerabilitate din sistemul Windows pentru a obține drepturi de administrator și ulterior, se propagă lateral către serverele critice. Un astfel de atac se poate desfășura în câteva minute, în timp ce detecția poate avea loc după săptămâni sau chiar luni.

2.11. Amenințări emergente

***Noile tehnologii contribuie la apariția unor amenințări cibernetice emergente**: IA, dispozitivele IoT integrate în infrastructura urbană și tehnologia deepfake, care permit atacatorilor să lanseze campanii de atac ultra-personalizate, să compromită rețelele smart-city și să falsifice conținut audio-video cu efecte reputaționale și operaționale importante.*

Discuția despre amenințările cibernetice nu poate fi completă fără a aborda riscurile emergente care, deși par, la prima vedere, de domeniul viitorului, sunt deja prezente în peisajul digital actual.

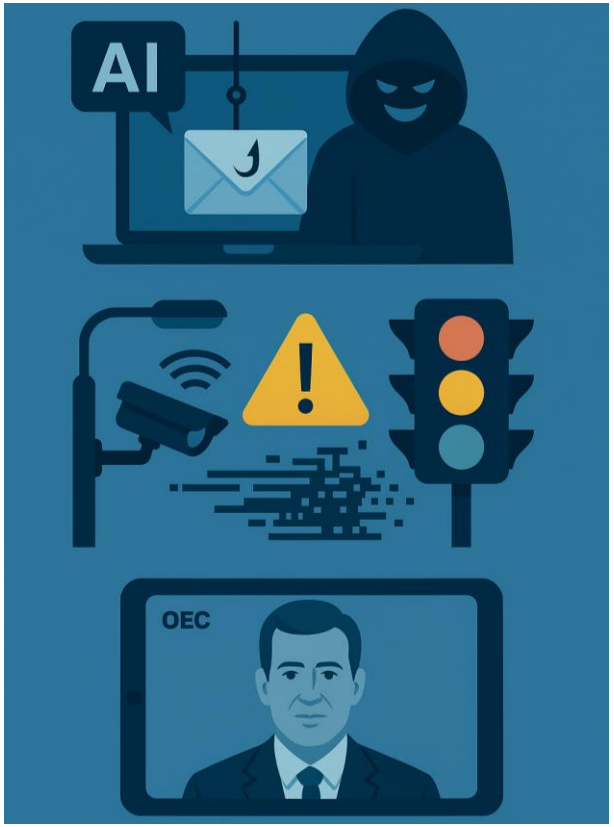
Inteligența artificială (IA) a democratizat accesul la atacuri cibernetice sofisticate. Astăzi, un atacator fără competențe tehnice avansate poate utiliza instrumente bazate pe IA pentru a genera automat e-mailuri de phishing personalizate, adaptate pentru fiecare angajat al unei primării. Aceste instrumente pot analiza stilul de comunicare regăsit în anunțurile publice și pot crea imagini sau videoclipuri false, în care primarul sau alți oficiali apar în contexte compromițătoare. IA este capabilă să genereze documente oficiale false, greu de deosebit de cele autentice, ceea ce sporește semnificativ riscurile pentru instituții.

Internet of Things (IoT) municipal aduce milioane de noi puncte de vulnerabilitate în mediul urban. Dispozitive precum senzori de monitorizare a calității aerului, camere de supraveghere inteligente, sisteme de semaforizare adaptivă sau stații de încărcare pentru vehicule electrice sunt conectate la Internet. Multe dintre aceste echipamente sunt implementate fără măsuri adecvate de securitate sau cu un nivel minim de protecție. Compromiterea unei rețele de senzori poate permite atacatorilor să acceseze date despre activitatea urbană, să manipuleze informațiile referitoare la trafic sau la calitatea aerului ori să influențeze deciziile administrative bazate pe aceste date.

Deepfake-urile video reprezintă o amenințare din ce în ce mai greu de contracarat. Impactul unor înregistrări false, în care primarul ar face declarații controversate în ajunul alegerilor locale, poate fi devastator. Chiar dacă ulterior frauda este demascată, consecințele asupra imaginii instituției și a încrederii publice pot fi ireversibile.

Atacurile asupra **stațiilor de încărcare pentru vehicule electrice** pot părea, la prima vedere, exotice, însă ele constituie deja o realitate. Aceste stații colectează date despre utilizatori, gestionează plăți electronice și sunt conectate la rețeaua electrică locală. Vulnerabilitățile existente în infrastructura acestora pot permite furtul datelor de plată, manipularea tarifelor aplicate sau chiar sabotarea funcționării rețelei electrice locale.

Riscurile asociate acestor amenințări emergente sunt îngrijorătoare deoarece infractorii cibernetici ar putea compromite sistemele de management al traficului dintr-un oraș și provoca blocaje severe în orele de vârf, prin modificarea timpilor semafoarelor. Astfel de atacuri pot rămâne nedetectate mai multe zile, până când autoritățile constată că schimbările nu au fost operate de personalul autorizat.



Figură 11. Amenințări emergente în spațiul digital

Exemplu: în anul 2024, mai multe instituții publice din UE au raportat tentative de phishing avansat în care mesajele erau redactate cu o coerență și adaptare contextuală specifică limbajului administrativ. Investigațiile au arătat că atacatorii au folosit modele de IA generativă pentru a personaliza conținutul mesajelor, simulând stilul oficial al corespondenței guvernamentale. Astfel de atacuri nu mai pot fi identificate ușor prin greșeli gramaticale sau formulări suspecte, așa cum se întâmpla frecvent în trecut.

3. MĂSURI DE PROTECȚIE

Într-un context administrativ tot mai complex și expus diverselor amenințări, implementarea unor măsuri de protecție eficiente în cadrul administrației publice locale devine primordială pentru asigurarea bunei funcționări a instituțiilor și pentru protejarea interesului public.

3.1. Principii generale de securitate

Securitatea cibernetică în administrația publică locală nu este doar o responsabilitate tehnică, ci ține de întreaga organizație. Cultura organizațională trebuie să includă respectul pentru reguli, atenția la detalii și asumarea responsabilității pentru protejarea informațiilor.

Instituțiile publice trebuie să promoveze un mediu în care angajații:

- **conștientizează** riscurile asociate activităților digitale;
- **raportează** fără teamă incidentele suspecte;
- **înțeleg** că fiecare persoană poate reprezenta o verigă slabă sau, dimpotrivă, un element de protecție în fața atacurilor cibernetice.

Pentru a proteja eficient informațiile și sistemele informatice, instituțiile publice trebuie să stabilească responsabilități clare în domeniul securității cibernetice:

- **desemnarea** persoanelor responsabile pentru implementarea și monitorizarea măsurilor de securitate;
- **stabilirea** unor proceduri scrise pentru gestionarea incidentelor de securitate;
- **instruirea** periodică a angajaților în privința obligațiilor lor legate de protecția datelor și a sistemelor informatice;
- **stabilirea** unui flux clar de raportare a incidentelor sau a situațiilor suspecte.

Instituțiile publice locale trebuie să aplice reguli de bază de igienă cibernetică, care să fie respectate de toți angajații, indiferent de funcție sau nivel de pregătire tehnică. Aceste reguli contribuie la reducerea semnificativă a riscurilor și includ:

- utilizarea de **parole complexe și unice** pentru fiecare cont utilizat în activitatea profesională;
- implementarea unei politici clare de **resetare a parolelor**, care să includă:
  - schimbarea periodică a parolelor (ex. la fiecare 90 de zile);
  - obligativitatea resetării parolei în cazul unui incident sau al suspiciunii de compromitere.
- **interzicerea** utilizării conturilor personale pentru activități instituționale;
- **atenția sporită** la e-mailuri sau mesaje suspecte care solicită informații confidențiale;
- **blocarea ecranului** calculatorului atunci când persoana părăsește biroul, chiar și pentru scurt timp;
- **interzicerea** conectării dispozitivelor USB necunoscute la echipamentele instituției;
- **verificarea sursei** programelor înainte de a le instala pe computerele instituției.

⚠ *Riscuri posibile:*

- *lipsa unei culturi organizaționale în care securitatea cibernetică este tratată ca o responsabilitate comună;*
- *absența procedurilor documentate pentru raportarea incidentelor și atribuirea responsabilităților;*
- *folosirea necontrolată a conturilor personale pentru sarcini profesionale;*
- *practici slabe de gestionare a parolelor (ex. reutilizarea sau partajarea acestora);*
- *lipsa unor controale minime privind dispozitivele externe și aplicațiile instalate;*
- *trivializarea instruirilor periodice, fără ancorare în riscurile reale sau exemple aplicabile.*

✅ *Acțiuni necesare:*

- *instituția trebuie să definească o politică oficială privind cultura de securitate, susținută la nivel managerial;*
- *se impune adoptarea unei politici unificate privind parolele, conturile utilizatorilor și restricțiile asupra dispozitivelor portabile;*
- *procedurile pentru raportarea incidentelor și atribuirea de responsabilități trebuie formalizate și comunicate întregului personal;*
- *se recomandă introducerea unor sesiuni lunare scurte de reîmprospătare a cunoștințelor privind igiena cibernetică;*
- *instruirea personalului trebuie să includă exemple concrete, adaptate contextului instituțional;*
- *este esențială auditarea periodică a practicilor de lucru, pentru a corecta eventualele abateri de la reguli.*

3.2. Măsuri pentru protecția conturilor și autentificării

Conturile de utilizator sunt poarta de intrare către informațiile și sistemele unei instituții, așa că e important să fie gestionate corect, ca să nu ajungă în mâinile cui nu trebuie. Dacă sunt administrate defectuos, pot fi afectate date sensibile, aplicații interne sau accesul la servicii esențiale.

Instituțiile trebuie să adopte politici clare pentru a reduce riscurile asociate cu parolele slabe sau reutilizate:

- parolele trebuie să aibă minimum 12 caractere, incluzând litere mari/mici, cifre și simboluri;
- este interzisă utilizarea de parole previzibile (ex. „Primaria123”);
- parolele nu trebuie reutilizate la conturi diferite și nu trebuie notate pe hârtie sau salvate în documente nesecurizate;
- parolele trebuie schimbate imediat în cazul unei suspiciuni de compromitere.

Autentificarea multi-factor (MFA) adaugă un nivel suplimentar de protecție, solicitând utilizatorului, pe lângă parolă, un al doilea element de verificare. Acesta poate fi un cod generat pe telefon, o aplicație de autentificare, un token fizic sau date biometrice:

- MFA este obligatorie pentru conturile cu acces la date sensibile sau sisteme critice (e-mail, aplicații de management al documentelor, platforme financiare);
- codurile de rezervă nu trebuie stocate în fișiere neprotejate. Acestea trebuie păstrate într-un spațiu securizat, accesibil doar titularului;
- angajații trebuie instruiți cum să utilizeze corect aplicațiile de autentificare și trebuie să cunoască procedura de recuperare în caz de pierdere a dispozitivului.

O bună administrare a conturilor reduce suprafața de atac și limitează impactul unei potențiale compromiteri:

- conturile neutilizate trebuie dezactivate imediat după plecarea unui angajat;
- utilizarea conturilor partajate trebuie evitată; fiecare angajat trebuie să aibă un cont individual;
- drepturile de acces se acordă în funcție de responsabilități, conform principiului „necesității de a cunoaște”;
- auditurile periodice ale conturilor sunt necesare pentru a identifica utilizatorii inactivi sau drepturile nejustificate.

⚠ *Riscuri posibile:*

- *un cont compromis oferă acces direct la sistemele interne, fără declanșarea unor alerte evidente;*
- *parolele slabe sau reutilizate pot fi ghicite ușor sau deja expuse în breșe anterioare;*
- *lipsa autentificării MFA permite atacatorilor să intre doar cu o parolă furată;*
- *codurile de rezervă salvate în clar pot fi accesate în caz de compromitere a stației de lucru;*
- *conturile vechi, neutilizate, rămân active și pot fi exploatate discret;*
- *utilizarea de conturi partajate face imposibilă trasabilitatea acțiunilor și împiedică reacția rapidă în caz de incident.*

✅ *Acțiuni necesare:*

- *configurează reguli tehnice care impun complexitatea minimă a parolelor și interzic reutilizarea acestora;*
- *activează MFA pentru toate conturile critice și asigură o procedură standard de resetare securizată;*
- *restricționează stocarea locală a codurilor MFA și oferă alternative sigure de backup;*
- *revizuiește periodic conturile active și revocă imediat accesul celor care nu mai au nevoie justificată;*
- *instruiește personalul să gestioneze responsabil informațiile de autentificare și să raporteze prompt orice suspiciune.*

3.3. Protecția echipamentelor și rețelei interne

Protejarea infrastructurii digitale este de maximă importanță pentru a asigura continuitatea serviciilor și securitatea datelor unei instituții publice. Vulnerabilitățile din rețeaua internă și de pe echipamente pot compromite informații sensibile și pot duce la întreruperea activităților zilnice. Pentru a consolida apărarea împotriva amenințărilor cibernetice, sunt necesare următoarele măsuri:

- actualizarea constantă a sistemelor informatice este una dintre cele mai simple și eficiente metode de a reduce riscurile cibernetice. O strategie eficientă de gestionare a actualizărilor trebuie să includă aplicarea imediată a corecțiilor critice de securitate, stabilirea unui calendar clar de actualizări și desemnarea unei persoane sau a unui departament responsabil de acest proces;
- segmentarea rețelei reprezintă împărțirea logică a rețelei interne în zone izolate (VLAN-uri), o abordare care limitează mișcarea laterală a unui atacator în cazul în care o parte a rețelei este compromisă. Este recomandată crearea de rețele separate pentru activitatea administrativă internă, pentru rețeaua destinată vizitatorilor și pentru echipamentele de tip IoT (camere video, senzori etc.);
- comunicarea în rețea trebuie să folosească exclusiv protocoale moderne și securizate, deoarece cele învechite sunt o sursă majoră de vulnerabilități. Recomandările includ dezactivarea completă a protocoalelor nesigure (precum SMBv1), folosirea exclusivă a HTTPS pentru traficul web și utilizarea TLS (Transport Layer Security) pentru criptarea comunicațiilor prin e-mail. De asemenea, este necesară protejarea suplimentară a serviciilor interne expuse pe Internet prin VPN-uri moderne și autentificare multi-factor (MFA);
- permisiunea de a folosi dispozitive personale (BYOD) la locul de muncă poate crește riscurile de securitate, deoarece aceste echipamente nu beneficiază de același nivel de control și protecție ca cele ale instituției. Măsurile recomandate sunt implementarea unei politici clare care să reglementeze utilizarea dispozitivelor personale în rețea, interzicerea stocării de date sensibile pe acestea fără o protecție adecvată și instalarea de soluții de securitate (antivirus, Mobile Device Management – MDM) pe dispozitivele folosite în scop profesional.

⚠ *Riscuri posibile:*

- *rețeaua instituției nu este segmentată, iar compromiterea unui echipament afectează toate celelalte sisteme conectate;*
- *protocoalele de comunicare nesecurizate permit interceptarea datelor transmise între angajați sau către servere externe;*
- *un angajat folosește laptopul personal, fără protecție antivirus sau criptare, pentru a accesa sistemele instituției;*
- *dispozitivele IoT (camere, senzori) sunt conectate direct în rețeaua principală, fără controale de securitate.*

✅ *Acțiuni necesare:*

- *actualizări periodice, testate preliminar pe un sistem dedicat;*
- *rețeaua internă ar trebui segmentată logic, cu politici stricte de acces și monitorizare a traficului;*
- *protocoalele învechite (ex. SMBv1) trebuie eliminate, iar comunicațiile securizate (HTTPS, TLS, VPN) utilizate exclusiv;*
- *politica BYOD trebuie să includă cerințe clare privind securitatea dispozitivelor personale (aplicații de protecție, criptare, autentificare);*
- *conectarea echipamentelor personale la rețeaua instituției ar trebui condiționată de aprobarea prealabilă a departamentului IT;*
- *este indicată utilizarea unei rețele separate pentru dispozitive IoT, izolată de infrastructura administrativă;*
- *personalul trebuie instruit periodic privind riscurile asociate și bunele practici de utilizare a echipamentelor IT.*

3.4. Securitatea serviciilor cloud

Utilizarea serviciilor de tip cloud, cum ar fi Google Drive și OneDrive, a crescut semnificativ în administrația publică, datorită beneficiilor precum facilitarea colaborării, accesul rapid la date și eficientizarea costurilor. Cu toate acestea, adoptarea acestor soluții aduce cu sine riscuri considerabile legate de securitatea datelor și conformitatea cu cerințele legale. O eroare frecventă în utilizarea serviciilor cloud constă în configurarea incorectă a permisiunilor de acces, ceea ce poate duce la expunerea neintenționată a documentelor.

Drepturile de acces trebuie acordate strict pe baza atribuțiilor de serviciu, iar setarea documentelor ca „Public" sau „Anyone with the link" este interzisă fără o aprobare justificată. Permisiunile de acces trebuie revizuite periodic pentru a se asigura că sunt aliniate cu rolurile actuale ale angajaților. Totodată, este recomandată activarea log-urilor pentru urmărirea accesărilor și protejarea accesului la conturi cu parole complexe și autentificare multi-factor (MFA).

Shadow IT constituie o provocare pentru administrația publică, deoarece se referă la utilizarea de către angajați a unor aplicații, platforme cloud sau dispozitive neautorizate în scopuri profesionale. Această practică expune instituția la riscuri considerabile, cum ar fi stocarea datelor pe servere private, necontrolate, și expunerea informațiilor în urma compromiterii conturilor personale.

Pentru a combate fenomenul de Shadow IT, este esențială definirea clară a aplicațiilor și platformelor cloud permise pentru uz profesional. Instalarea de software neaprobat trebuie restricționată prin politici de grup (GPO) sau prin limitarea conturilor utilizatorilor. De asemenea, se recomandă utilizarea soluțiilor de Mobile Device Management (MDM) pentru gestionarea securizată a dispozitivelor mobile. Instituțiile trebuie să efectueze audituri periodice ale rețelei pentru a identifica soluțiile neautorizate și să instruiască angajații cu privire la riscurile aplicațiilor externe, subliniind importanța utilizării soluțiilor oficiale.

Conform GDPR, instituțiile publice au responsabilități stricte în utilizarea serviciilor cloud. Nerespectarea acestor cerințe poate atrage sancțiuni considerabile, de până la 4% din bugetul anual al instituției. Aceste responsabilități includ asigurarea că datele personale nu sunt stocate în afara UE fără garanții contractuale adecvate. De asemenea, instituția trebuie să aibă o vizibilitate clară asupra locației și modului în care sunt stocate datele, să încheie contracte cu furnizorii de servicii cloud care includ clauze de protecție a datelor și să raporteze incidentele de securitate conform cerințelor GDPR, în special dacă sunt implicate date personale.

⚠️ *Riscuri posibile:*

- *documente sensibile devin accesibile din cauza configurărilor incorecte;*
- *angajații utilizează platforme cloud sau aplicații neautorizate pentru activități profesionale;*
- *lipsa vizibilității asupra locației și modului de stocare a datelor personale;*
- *conturile cloud fără protecție adecvată pot fi compromise ușor;*
- *instituția nu poate demonstra conformitatea cu cerințele legale privind protecția datelor.*

✅ *Acțiuni necesare:*

- *stabilește politici clare privind utilizarea serviciilor cloud, accesul la documente și partajarea de fișiere;*
- *aprobă doar platforme conforme cu cerințele de securitate și legislația în vigoare;*
- *activează autentificarea multi-factor și jurnalizarea accesărilor pentru conturile cloud;*
- *interzice utilizarea aplicațiilor externe neaprobate în lipsa unei evaluări de securitate;*
- *oferă angajaților soluții oficiale și instruire periodică privind utilizarea responsabilă a serviciilor online;*
- *asigură contracte clare cu furnizorii de servicii cloud, cu precizarea locației datelor și a obligațiilor de confidențialitate;*
- *monitorizează constant utilizarea resurselor cloud și documentează orice incident de securitate.*

3.5. Securitatea aplicațiilor web

Site-urile și aplicațiile web ale administrației publice locale reprezintă poarta digitală de acces a cetățenilor la servicii publice. Vulnerabilitățile acestor platforme pot compromite date cu caracter personal, afecta imaginea instituției și întrerupe furnizarea serviciilor esențiale. Din acest motiv, securitatea trebuie tratată ca o responsabilitate continuă, nu doar ca o etapă din procesul de dezvoltare.

Indiferent dacă aplicațiile sunt dezvoltate de personalul intern sau de furnizori externi, trebuie respectate standarde minime de securitate, printre care:

- codul sursă trebuie să respecte recomandările OWASP Top 10 [9] (ex. injecții SQL, XSS, CSRF);
- toate datele introduse de utilizatori trebuie validate și filtrate înainte de procesare;
- parolele și datele sensibile nu se stochează în clar în baze de date;
- mesajele de eroare nu trebuie să conțină detalii tehnice despre aplicație;
- zonele de administrare trebuie protejate prin autentificare puternică (ideal cu MFA) și acces restricționat.

Testarea de securitate trebuie planificată pe tot parcursul ciclului de viață al aplicației, prin:

- scanări automate periodice pentru identificarea vulnerabilităților cunoscute;
- audituri de securitate realizate de firme specializate, în cazul aplicațiilor critice;
- reverificarea securității după orice actualizare majoră sau modificare de funcționalitate;
- instituția trebuie să solicite dezvoltatorilor dovezi clare privind testarea și conformitatea aplicației (ex. rapoarte, certificate).

Site-ul instituției nu este doar o platformă de informare, ci și o componentă de bază a încrederii publice:

- comunicarea între utilizatori și site trebuie realizată exclusiv prin HTTPS;
- zona de administrare nu trebuie să fie accesibilă publicului și nici ușor de identificat (ex. /admin, /wp-admin);
- accesul la platforma de administrare trebuie securizat cu autentificare robustă și limitat la personal autorizat;
- sistemele de backup trebuie configurate și testate periodic, iar copiile de siguranță păstrate în locații sigure;
- actualizările platformei (ex. CMS) și ale extensiilor trebuie aplicate imediat ce devin disponibile;
- conturile de administrare trebuie să fie individuale, să aibă parole complexe și să nu fie partajate.

⚠ *Riscuri posibile:*

- *aplicațiile web conțin vulnerabilități critice din cauza codului nesecurizat sau a lipsei testării;*
- *datele cetățenilor pot fi expuse din cauza unei autentificări slabe sau a parolelor stocate necorespunzător;*
- *zona de administrare a site-ului poate fi accesată neautorizat din lipsa restricțiilor și a autentificării multi-factor;*
- *lipsa actualizărilor permite exploatarea unor vulnerabilități cunoscute;*
- *platformele dezvoltate extern nu sunt auditate de instituție înainte de lansare.*

✅ *Acțiuni necesare:*

- *testarea de securitate trebuie integrată ca etapă obligatorie în toate fazele proiectelor web, de la dezvoltare până la implementare și actualizare;*
- *dezvoltatorii trebuie să furnizeze documente care atestă efectuarea testărilor de securitate (scanări, rapoarte tehnice, certificate de conformitate);*
- *accesul la interfața de administrare a site-ului trebuie să fie restricționat, ascuns și protejat prin autentificare puternică, de preferat cu mecanisme multi-factor (MFA);*
- *backup-urile site-ului trebuie realizate periodic și stocate în locații separate, cu nivel ridicat de securitate;*
- *platformele utilizate (ex. CMS, module, plugin-uri) trebuie actualizate fără întârziere, imediat ce sunt disponibile patch-uri de securitate;*
- *trebuie elaborat și menținut un plan instituțional de răspuns la incidente de securitate cibernetică ce implică aplicații web sau site-ul oficial.*

3.6. Protecția împotriva ransomware și malware

Prevenirea și gestionarea riscurilor asociate cu ransomware-ul și alte forme de malware necesită măsuri tehnice și organizatorice aplicabile la nivelul întregii infrastructuri IT și al tuturor angajaților. O singură compromitere poate bloca accesul la documente esențiale, perturba funcționarea instituției și afecta serviciile pentru cetățeni.

Backup-ul reprezintă cea mai eficientă metodă de a limita impactul unui atac reușit. Fără copii de siguranță funcționale, datele instituției pot fi pierdute definitiv:

- backup-urile trebuie realizate periodic, zilnic sau săptămânal, în funcție de volumul și importanța datelor gestionate;
- cel puțin o copie de rezervă trebuie păstrată offline sau într-o locație izolată de rețea, pentru a evita criptarea simultană a datelor și a backup-urilor;
- testarea periodică a backup-urilor este importantă pentru a confirma posibilitatea restaurării corecte a datelor;
- responsabilitățile privind backup-ul și procedurile de restaurare trebuie definite clar, într-un cadru documentat și verificabil.

Ransomware-ul se poate răspândi rapid dacă utilizatorii dispun de drepturi de acces excesive. Pentru a limita riscurile:

- conturile de utilizator trebuie să aibă doar permisiuni minime, adaptate nevoilor reale ale fiecărui post;
- conturile de administrator nu trebuie utilizate pentru activități curente, cum ar fi navigarea pe Internet sau trimiterea de e-mailuri;
- accesul la directoarele sensibile trebuie justificat și limitat, iar o evidență clară a conturilor privilegiate și a modificărilor de acces trebuie păstrată;
- auditurile periodice sunt necesare pentru a revizui și a elimina drepturile nejustificate.

O capacitate de reacție rapidă este crucială pentru a limita efectele unui atac:

- toate echipamentele trebuie protejate cu soluții antivirus și anti-malware actualizate. Soluțiile EDR (Endpoint Detection and Response) sunt recomandate pentru identificarea și izolarea comportamentelor suspecte;
- o procedură clară de raportare a incidentelor trebuie implementată și cunoscută de toți angajații;
- în cazul unei posibile infectări, dispozitivul afectat trebuie deconectat imediat de la rețea, iar incidentul trebuie raportat persoanei responsabile cu securitatea IT;
- Păstrarea jurnalelor de sistem (log-uri) este necesară pentru a investiga sursa atacurilor, iar o analiză post-incident este obligatorie pentru a îmbunătăți măsurile de protecție.

⚠️ *Riscuri posibile:*

- *blocarea totală a accesului la documente, aplicații și sisteme esențiale pentru funcționarea instituției;*
- *răspândirea malware-ului în întreaga rețea prin conturi cu drepturi extinse sau prin lipsa segmentării;*
- *pierderea definitivă a datelor în absența unor copii de rezervă funcționale și testate;*
- *expunerea la sancțiuni legale sau reputaționale în cazul compromiterii datelor sensibile ale cetățenilor.*

✅ *Acțiuni necesare:*

- *stabilește politici clare de backup, care să includă frecvența salvării, locația copiilor și responsabilitățile tehnice;*
- *păstrează cel puțin o copie de rezervă offline sau în infrastructuri izolate și testează periodic capacitatea de restaurare;*
- *asigură limitarea drepturilor de acces la strictul necesar fiecărui post, prin conturi individuale și monitorizate;*
- *utilizează soluții antivirus și EDR actualizate, capabile să identifice, să alerteze și să izoleze rapid comportamentele anormale;*
- *definește o procedură internă de raportare a incidentelor, cunoscută de tot personalul instituției;*
- *realizează o analiză tehnică și organizațională după fiecare incident pentru a îmbunătăți măsurile de protecție existente.*

3.7. Conștientizarea și instruirea personalului

Securitatea cibernetică depinde în mare măsură de comportamentul angajaților, nu doar de tehnologie. Majoritatea atacurilor cibernetice reușesc deoarece angajații sunt induși în eroare să divulge informații sau să deschidă fișiere periculoase. Prin instruire continuă, instituțiile publice pot transforma angajații dintr-o vulnerabilitate într-o linie de apărare.

Conștientizarea personalului este esențială pentru a preveni riscuri majore, cum ar fi blocarea completă a accesului la documente prin criptare, pierderea ireversibilă a datelor (în lipsa unor backup-uri funcționale) și răspândirea malware-ului în rețea prin conturi cu drepturi excesive. O instruire eficientă reduce, de asemenea, riscul de întrerupere a activității instituției și de scădere a încrederii publicului în urma unui incident mediatizat.

Atacurile de tip phishing și inginerie socială vizează direct angajații, exploatând încrederea, graba sau lipsa de informare. Angajații trebuie instruiți să recunoască semnele care indică o potențială amenințare, cum ar fi mesajele ce creează urgență, erorile gramaticale, solicitările de date personale sau link-urile către site-uri necunoscute.

Pe lângă regulile teoretice, instituțiile trebuie să organizeze periodic exerciții practice pentru a simula atacuri și a evalua reacțiile angajaților. Acestea pot include campanii simulate de phishing sau jocuri de rol. O altă măsură eficientă este analiza incidentelor reale din alte instituții, pentru a învăța lecții concrete și a preveni evenimente similare. Reducerea riscurilor cibernetice necesită respectarea constantă a unor reguli simple, cum ar fi blocarea ecranului calculatorului când biroul este părăsit, utilizarea de parole complexe, evitarea conectării dispozitivelor USB necunoscute și instalarea de programe software doar cu aprobarea departamentului IT.

Instituțiile trebuie să dezvolte o cultură organizațională în care securitatea este o responsabilitate comună, iar angajații raportează fără teamă incidentele suspecte. Un plan de instruire continuă și adaptat riscurilor reale asigură că fiecare angajat devine un element de protecție. Este vital ca personalul să înțeleagă că fiecare acțiune, chiar și cele minore, poate avea un impact semnificativ asupra securității instituției. Măsurile de instruire, dublate de o politică internă solidă, transformă angajații în prima linie de apărare, reducând drastic șansele ca un atac să aibă succes.

⚠ *Riscuri posibile:*

- *Angajații pot fi induși în eroare de atacurile de tip phishing să dezvăluie parole sau alte date de autentificare, permițând atacatorilor acces neautorizat la sistemele instituției;*
- *Un singur angajat poate introduce un virus în rețea prin deschiderea de fișiere periculoase sau accesarea de link-uri malițioase, ceea ce poate duce la o răspândire rapidă a malware-ului;*
- *Nerespectarea regulilor de igienă cibernetică, cum ar fi utilizarea unor stick-uri USB necunoscute, poate duce la pierderea de informații sensibile sau la compromiterea integrității datelor;*
- *Un incident cibernetic major, cauzat de lipsa de instruire a personalului, poate afecta grav încrederea publicului în capacitatea instituției de a proteja informațiile cetățenilor.*

✅ *Acțiuni necesare:*

- *Crearea unei culturi de securitate, prin care angajații sunt încurajați să raporteze fără teamă incidentele suspecte, este esențială pentru a preveni pagube majore;*
- *Instituția trebuie să asigure o instruire periodică și adaptată riscurilor specifice, care să includă exerciții practice pentru a îmbunătăți reacțiile angajaților;*
- *Se impune definirea unui flux clar de comunicare, astfel încât fiecare angajat să știe cui să raporteze un eveniment suspect și ce pași să urmeze pentru a limita răspândirea unei amenințări.*

3.8. Managementul dispozitivelor portabile și mobile

Importanța protecției dispozitivelor portabile. Dispozitivele portabile (cum ar fi stick-urile USB, telefoanele mobile sau hard disk-urile externe) sunt instrumente esențiale în activitatea instituțiilor publice, facilitând transferul rapid de fișiere și munca la distanță. Cu toate acestea, ele prezintă un risc sporit pentru securitatea informațiilor, deoarece pot fi ușor pierdute, furate sau compromise. Un incident care implică aceste echipamente poate duce la scurgerea, modificarea sau pierderea definitivă a datelor instituționale, afectând continuitatea activității și imaginea publică.

Stick-uri USB și medii de stocare externe. Aceste medii de stocare sunt printre cele mai expuse la amenințări cibernetice. Atacatorii pot modifica un dispozitiv USB pentru a executa comenzi malițioase imediat după conectare. În plus, stick-urile pot fi folosite ca vectori pentru propagarea de malware, iar utilizarea lor fără verificări prealabile crește considerabil riscul de compromitere a datelor.

Telefoanele mobile. Utilizarea telefoanelor mobile în scop profesional implică gestionarea de e-mailuri și documente, ceea ce le transformă în ținte atractive pentru atacatori. Pierderea sau furtul dispozitivului poate facilita accesul neautorizat la informații sensibile, iar instalarea de aplicații necontrolate sau conectarea la rețele Wi-Fi nesecurizate poate compromite întreaga infrastructură instituțională.

Gestionarea centralizată a dispozitivelor. Lipsa unei politici clare privind administrarea echipamentelor portabile îngreunează controlul accesului și al actualizărilor de securitate. Un management eficient presupune inventarierea tuturor dispozitivelor, stabilirea nivelurilor de acces, implementarea măsurilor de criptare și aplicarea constantă a actualizărilor de securitate.

Bune practici generale. Dispozitivele portabile care conțin date instituționale trebuie păstrate în spații sigure și monitorizate. Criptarea datelor, restricționarea utilizării în scop personal și raportarea imediată a pierderii sau furtului echipamentului sunt pași esențiali pentru reducerea riscurilor. De asemenea, instruirea personalului privind manipularea corectă a acestor dispozitive contribuie semnificativ la prevenirea incidentelor.

⚠ *Riscuri posibile:*

- *infectarea rețelei interne prin conectarea unui dispozitiv compromis;*
- *pierderea sau furtul echipamentului, cu acces direct la date sensibile;*
- *exfiltrarea neautorizată a documentelor stocate local;*
- *utilizarea de aplicații sau rețele nesecurizate care facilitează compromiterea conturilor;*
- *introducerea neintenționată de malware prin stick-uri USB sau carduri de memorie.*

✅ *Acțiuni necesare:*

- *asigurarea inventarierii și monitorizării tuturor dispozitivelor portabile utilizate în instituție;*
- *criptarea obligatorie a datelor stocate pe medii mobile și protejarea cu parole complexe sau metode biometrice;*
- *aplicarea politicilor tehnice de restricționare a porturilor USB acolo unde nu sunt necesare;*
- *scanarea automată a mediilor externe înainte de accesarea fișierelor;*
- *limitarea utilizării dispozitivelor portabile la activități strict instituționale;*
- *raportarea imediată a pierderii sau furtului echipamentului către responsabilul IT;*
- *instruirea periodică a personalului privind riscurile și practicile corecte de manipulare a echipamentelor mobile.*

3.9. Măsuri pentru amenințările emergente

Evoluția tehnologică aduce beneficii semnificative, dar creează și noi riscuri cibernetice pentru administrația publică. Tehnologii precum IA, dispozitivele IoT și tehnologiile deepfake extind considerabil suprafața de atac, generând scenarii care nu existau în trecut. Pentru a gestiona aceste riscuri, este necesară o abordare proactivă, concentrată pe implementarea de măsuri de protecție.

Protecția împotriva dezinformării bazate pe IA și deepfake. Atacatorii utilizează IA pentru a automatiza și personaliza atacuri, generând campanii de phishing convingătoare sau documente oficiale false. De asemenea, tehnologia deepfake permite crearea de materiale audio sau video extrem de realiste, folosite pentru a disemina dezinformare și a afecta credibilitatea instituției.

Măsuri de protecție:

- stabilirea unor proceduri clare de verificare a autenticității materialelor audio-video înainte de difuzare;
- implementarea unor programe periodice de instruire a personalului pentru a recunoaște și raporta conținuturile suspecte;
- aplicarea verificării duble pentru solicitările sensibile și tranzacțiile cu risc ridicat, în special cele care par a veni din partea conducerii;
- integrarea monitorizării active a mediului online și a rețelelor sociale pentru detectarea rapidă a campaniilor de dezinformare.

Securizarea infrastructurii inteligente. Dispozitivele IoT, precum camerele de supraveghere și senzorii de mediu, aduc numeroase beneficii, dar pot deveni puncte de vulnerabilitate dacă nu sunt securizate corespunzător. Compromiterea lor poate duce la accesarea neautorizată a rețelelor interne sau la manipularea datelor. Pentru a preveni aceste riscuri, este important să se implementeze:

- segmentarea și izolarea rețelelor care găzduiesc dispozitive IoT de infrastructura administrativă;
- actualizarea constantă a politicilor de securitate în funcție de evoluția tehnologică;
- asigurarea că toate echipamentele IoT sunt configurate cu măsuri adecvate de securitate încă din faza de implementare.

Prin integrarea acestor măsuri, instituțiile publice pot construi servicii moderne, eficiente și reziliente, care să servească în mod responsabil interesele cetățenilor și ale comunității.

⚠ *Riscuri posibile:*

- *crearea și distribuirea de materiale deepfake care pot induce în eroare publicul și compromite credibilitatea instituției;*
- *lansarea de atacuri cibernetice avansate, personalizate cu ajutorul inteligenței artificiale;*
- *exploatarea dispozitivelor IoT pentru acces neautorizat la rețelele interne;*
- *utilizarea tehnologiilor emergente pentru colectarea și manipularea datelor sensibile;*
- *afectarea proceselor administrative și a serviciilor publice esențiale în urma unor atacuri coordonate.*

✅ *Acțiuni necesare:*

- *implementarea unor programe periodice de instruire privind identificarea și raportarea amenințărilor emergente;*
- *stabilirea unor proceduri clare de verificare a autenticității materialelor audio-video înainte de difuzare;*
- *aplicarea verificării duble pentru solicitările sensibile și tranzacțiile cu risc ridicat;*
- *integrarea monitorizării active a mediului online și a rețelelor sociale pentru detectarea rapidă a campaniilor de dezinformare;*
- *segmentarea și izolarea rețelelor care găzduiesc dispozitive IoT;*
- *actualizarea constantă a politicilor de securitate în funcție de evoluția tehnologică și a amenințărilor identificate.*

3.10. Răspuns la incidente și planuri de continuitate

Importanța reacției rapide la incidente. Nicio instituție publică nu este imună la atacuri cibernetice. Diferența dintre un incident minor și o criză majoră este determinată de rapiditatea și eficiența reacției. Prin urmare, este esențial să existe proceduri clare și personal instruit pentru a identifica incidentele, a limita pagubele, a comunica eficient și a asigura continuitatea activităților critice.

Gestionarea incidentelor. La detectarea unui incident, primul pas este izolarea imediată a sistemului afectat, prin deconectarea de la rețea (fie prin cablu, fie prin Wi-Fi). Este interzisă ștergerea fișierelor suspecte sau reinstalarea sistemului de operare înainte de o evaluare completă, pentru a nu compromite probele necesare analizei tehnice și juridice. Detaliile relevante (momentul apariției, mesajele afișate, acțiunile întreprinse anterior) trebuie consemnate cu acuratețe și transmise responsabilului IT/Cibernetic.

Limitarea impactului. În paralel, conturile afectate trebuie blocate, iar sistemele compromise izolate fizic și logic de restul infrastructurii. Echipa tehnică trebuie să fie alertată imediat, pentru a identifica natura și extinderea incidentului. În cazul atacurilor de tip ransomware, nu se răspunde solicitărilor de plată, fiind obligatorie implicarea autorităților competente și a echipei juridice.

Notificarea incidentului și obligațiile legale. Comunicarea este o componentă critică a managementului incidentelor. Instituția trebuie să stabilească în avans cine primește raportările inițiale, cine informează conducerea și autoritățile externe și cine transmite mesajele publice oficiale, pentru a evita informațiile contradictorii.

În cazul în care sunt implicate date cu caracter personal, incidentul trebuie raportat către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) în maximum 72 de ore de la constatare. Pentru incidente majore de securitate cibernetică, legislația poate impune raportarea către DNSC sau către alte autorități competente.

Planuri de continuitate. Instituțiile trebuie să identifice activitățile critice care nu pot fi întrerupte și să asigure resurse alternative. Datele esențiale trebuie protejate prin copii de siguranță păstrate în locații sigure și testate periodic. Este necesară existența unor proceduri pentru relocarea temporară a activităților și pentru funcționarea în condiții limitate. Instruirea personalului privind modul de lucru în regim de avarie este esențială pentru menținerea serviciilor publice și reducerea timpilor de nefuncționare.

⚠ *Riscuri posibile:*

- *extinderea rapidă a atacului în lipsa izolării imediate a sistemelor compromise;*
- *pierderea definitivă a datelor și întreruperea serviciilor publice;*
- *nerespectarea obligațiilor legale de raportare, cu sancțiuni corespunzătoare;*
- *creșterea impactului mediatic și afectarea încrederii publice;*
- *întârzierea reluării activităților critice din cauza lipsei unui plan de continuitate.*

✅ *Acțiuni necesare:*

- *stabilirea și testarea periodică a procedurilor de răspuns la incidente;*
- *asigurarea unei comunicări interne și externe structurate și rapide;*
- *menținerea unei evidențe actualizate a persoanelor responsabile și a fluxului de raportare;*
- *blocarea imediată a conturilor compromise și izolarea sistemelor afectate;*
- *păstrarea și testarea regulată a copiilor de siguranță ale datelor esențiale;*
- *revizuirea post-incident a proceselor și actualizarea planurilor de continuitate.*

4. ASPECTE LEGALE ȘI DE CONFORMITATE

Această secțiune oferă o prezentare consolidată și clară a cadrului normativ relevant, a obligațiilor legale și a implicațiilor pentru instituțiile publice locale.

4.1. Fluxuri de raportare către autoritățile competente

În cazul unui incident cibernetic sau al unei scurgeri de date personale, instituția trebuie să urmeze un flux de raportare. **Fluxul de raportare recomandat este**:

- incident cibernetic în care nu au fost compromise date cu caracter personal:
  - se raportează la DNSC.
- incident care **implică date personale** (ex. scurgere de date, e-mail greșit):
  - se notifică ANSPDCP în maximum 72 de ore;
  - se raportează și la DNSC dacă incidentul are impact asupra securității informatice.

Conducerea instituției trebuie să stabilească persoane clar desemnate pentru gestionarea acestor raportări. Respectarea legislației privind protecția datelor și securitatea cibernetică nu este opțională, aceasta protejează instituția, angajații și încrederea cetățenilor. Măsurile minime de conformitate pot fi implementate chiar și în condiții de buget restrânse.[10]

4.2. Responsabilități și bune practici de conformitate

Neconformitatea poate atrage sancțiuni, dar și pierderea încrederii cetățenilor în instituțiile publice. Tabelul de mai jos sintetizează obligațiile principale și persoanele desemnate ca responsabile în cadrul instituției:

Tabel 1. Responsabilități și sancțiuni asociate în contextul securității cibernetice

Domeniul	Responsabil	Sancțiuni posibile
Protecția datelor personale (GDPR)	Ofițerul de protecție a datelor (DPO)	Amenzi de până la 20 milioane € sau 4 % din cifra de afaceri globală anuală (oricare este mai mare), impuse de Autoritatea de Supraveghere pentru încălcări grave ale GDPR
Raportarea incidentelor cibernetice	Persoana desemnată pentru securitatea IT	Potrivit OUG 104/2021, DNSC nu are competența de a sancționa contravențional neraportarea incidentelor. Totuși, dacă sunt implicate date personale, se pot aplica sancțiuni conform GDPR sau altor reglementări naționale
Instruirea angajaților	Conducerea instituției, în colaborare cu DPO/IT	Deși legea nu prevede sancțiuni directe pentru absența sesiunilor de formare, lipsa instruirii crește riscul incidentelor cibernetice, cu posibile consecințe asupra imaginii instituției și costuri indirecte semnificative

Principalele acte normative relevante sunt:

- *Regulamentul General privind Protecția Datelor (GDPR): stabilește reguli stricte pentru protejarea datelor personale ale cetățenilor;*
- *OUG nr. 155/2024: transpune în legislația națională cerințele Directivei (UE) 2022/2555 (NIS2), extinzând domeniul de aplicare și consolidând obligațiile de securitate și raportare;*
- *Legea nr. 506/2004: reglementează prelucrarea datelor personale și protecția vieții private în sectorul comunicațiilor electronice;*
- *Alte Ordonanțe de Urgență și Hotărâri de Guvern: ce reglementează aspecte conexe de securitate cibernetică și digitalizarea administrației publice.*

Exemple:

- *datele personale nu trebuie publicate pe site-ul instituției fără un temei legal;*
- *orice incident de securitate care implică date cu caracter personal trebuie notificat Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) fără întârzieri nejustificate și, în orice caz, în maximum 72 de ore de la constatarea acestuia;*
- *dacă un angajat transmite din greșeală prin e-mail datele unui cetățean, instituția va notifica ANSPDCP în cel mult 72 de ore de la descoperirea incidentului;*
- *personalul instituției trebuie să verifice periodic cine are acces la datele cu caracter personal ale cetățenilor;*
- *nu toți angajații trebuie să aibă acces la bazele de date cu impozite și taxe.*

5. PROCEDURI DE MANAGEMENT AL INCIDENTELOR CIBERNETICE

Această secțiune stabilește proceduri clare, adaptate realității administrației publice locale, care să permită o reacție rapidă și coordonată.

5.1. Clasificarea și prioritizarea incidentelor

Nu toate incidentele cibernetice sunt la fel de grave. Unele pot fi rezolvate rapid, fără impact major, în timp ce altele pot afecta serviciile esențiale ale primăriei sau datele personale ale cetățenilor. Clasificarea rapidă a unui incident ajută instituția să înțeleagă gravitatea situației, să reacționeze proporțional și să aloce resursele adecvate pe baza următoarelor criterii:

- afectarea activității instituției:
  - sunt blocate servicii importante (ex. emiterea de documente pentru cetățeni)?
  - instituția își poate desfășura activitatea normal?
- afectarea datelor personale:
  - sunt implicate date ale cetățenilor sau ale angajaților?
  - există riscul ca aceste date să ajungă la alte persoane?
- răspândirea incidentului:
  - problema este limitată la un singur calculator sau afectează mai multe?
  - se propagă rapid în rețeaua internă?
- durata estimată a remedierii:
  - se poate rezolva în câteva ore?
  - este nevoie de mai multe zile sau chiar săptămâni pentru revenirea la normal?
- impactul asupra imaginii instituției:
  - dacă incidentul devine public, poate afecta încrederea cetățenilor?
  - pot apărea riscuri legale sau mediatice?

Tabel 2. Clasificarea incidentelor în funcție de severitate și impact operațional

Nivel	Descriere
Minor	Incident cu impact redus - activitatea instituției nu este afectată considerabil
Semnificativ	Incident cu impact mediu - necesită intervenție promptă, dar nu împiedică desfășurarea activităților curente
Critic	Incident cu impact major - compromite grav activitatea instituției sau datele personale, necesită intervenție imediată

Exemple de incidente:

- *antivirusul detectează și blochează automat un fișier malițios;*
- *un angajat primește un e-mail suspect, dar nu accesează link-ul și nu deschide atașamentele;*
- *un angajat apasă pe un link de phishing, dar nu completează datele personale;*
- *o secțiune a site-ului primăriei este inaccesibilă pentru o perioadă scurtă;*
- *un atac ransomware criptează și blochează calculatoarele;*
- *apare o scurgere de date cu caracter personal către terți;*
- *site-ul primăriei este modificat neautorizat cu conținut defăimător sau mesaje ilegale.*

Recomandări:

- *se va raporta imediat orice incident cibernetic suspect, indiferent de gravitate, către persoana responsabilă cu securitatea IT;*
- *persoana desemnată pentru securitate IT va clasifica incidentul în unul dintre nivelurile de prioritate stabilite;*
- *dacă incidentul implică date cu caracter personal, acesta se consideră automat de nivel semnificativ (sau critic) și va fi evaluat pentru notificarea ANSPDCP în termen de 72 de ore de la constatare.*

6. IMPLEMENTARE ȘI MONITORIZARE

Prezenta secțiune oferă un plan structurat pentru aplicarea recomandărilor, urmărirea progresului și adaptarea constantă la noile amenințări.

6.1. Etapele de implementare a măsurilor propuse

De ce sunt necesare etapele? Pentru că securitatea cibernetică nu se obține printr-o acțiune singulară, ci reprezintă un proces gradual care presupune planificare, implementare și verificare continuă:

1. evaluarea situației actuale (audit inițial):
   - se analizează starea curentă a infrastructurii IT și a măsurilor de securitate implementate;
   - se identifică punctele slabe și se prioritizează acțiunile;
   - se evaluează nivelul de instruire a personalului.
2. stabilirea priorităților:
   - măsurile sunt clasificate în funcție de urgență și impact:
     - critice - se implementează imediat (ex: parole complexe, backup, segmentarea rețelei);
     - importante - se realizează pe termen scurt (ex: testări periodice, audituri de securitate);
     - avansate - se planifică pe termen mediu sau lung (ex: soluții EDR, cursuri specializate).
3. elaborarea unui plan de acțiune:
   - se definesc clar măsurile de implementare, se stabilesc responsabilii pentru fiecare acțiune și se estimează bugetul necesar;
   - se stabilesc termenele de realizare pentru fiecare acțiune.
4. implementarea măsurilor:
   - parole complexe - responsabilul IT/Cibernetic, termen 30 de zile;
   - instruire anti-phishing - departamentul HR, în colaborare cu IT, termen 45 de zile;
   - segmentare rețea - responsabilul IT/Cibernetic, termen 60 de zile.
5. testare și verificare:
   - se evaluează dacă măsurile aplicate funcționează conform așteptărilor;
   - se testează funcționalitatea backup-urilor;
   - se rulează simulări de phishing pentru a evalua vigilența angajaților;
   - se verifică respectarea politicilor de parolă.
6. raportare și îmbunătățire continuă:
   - se prezintă periodic rapoarte conducerii instituției;
   - planul de măsuri este revizuit și actualizat în funcție de noile riscuri, recomandările DNSC și lecțiile învățate din incidentele recente.

Exemple:

- *primăria X a descoperit că parolele majorității angajaților erau simple și nu existau proceduri clare pentru reacția la incidente;*
- *instituția nu avea fonduri pentru soluții avansate, dar a început imediat cu segmentarea rețelei și instruirea angajaților;*
- *persoana desemnată pentru securitate IT a aplicat, prin politici de grup (Group Policy Object), restricții asupra claselor de dispozitive de stocare USB (Mass Storage Devices) pe stațiile de lucru administrative. Porturile USB au rămas active pentru periferice esențiale (tastatură, mouse), prevenind astfel riscul de infectare prin stick-uri, fără a afecta activitatea operațională;*
- *primăria a testat restaurarea backup-urilor și a descoperit că unele fișiere esențiale nu fuseseră salvate.*

6.2. Verificarea măsurilor implementate

După implementarea măsurilor de securitate, instituția trebuie să verifice periodic dacă acestea funcționează. Întrebările de mai jos pot ajuta la această verificare:

1. toți angajații știu cum să raporteze un incident?
2. există parole complexe pe toate conturile?
3. se realizează backup periodic și se testează restaurarea datelor?
4. rețeaua este segmentată între zona publică și cea administrativă?
5. a fost organizată cel puțin o instruire în ultimul an?
6. s-au aplicat ultimele actualizări de securitate la calculatoare și servere?

*Dacă răspunsul la oricare dintre aceste întrebări este „**NU**”, instituția ar trebui să ia măsuri imediat.*

6.3. Roluri și responsabilități

Securitatea cibernetică nu reprezintă exclusiv atribuția departamentului IT, ci o responsabilitate comună a întregului personal. Protejarea datelor și a infrastructurii informatice presupune implicarea tuturor angajaților. Pentru a asigura o reacție eficientă și coordonată, este esențial ca fiecare persoană să își cunoască clar rolul și responsabilitățile.

Conducerea instituției – responsabilități:

- aprobă politica de securitate cibernetică;
- asigură alocarea bugetului necesar;
- ia deciziile finale în cazul unui incident major;
- desemnează persoanele responsabile de securitate.

***Primarul** trebuie să conștientizeze că securitatea cibernetică implică întreaga organizație, nu doar departamentul IT.*

Responsabilul IT sau persoana desemnată cu securitatea informației – atribuții principale:

- implementează măsurile tehnice de securitate (parole, segmentare rețea etc.);
- monitorizează rețeaua și sistemele;
- gestionează incidentele cibernetice;
- ține legătura cu DNSC în cazul incidentelor majore;
- participă la instruirea angajaților.

***Responsabilul IT** sau persoana desemnată cu securitatea informației este persoana responsabilă cu identificarea și izolarea rapidă a unui echipament compromis, inclusiv deconectarea acestuia din rețea în cazul unei infectări.*

Responsabilul GDPR – responsabilități:

- verifică respectarea legislației privind protecția datelor personale;
- coordonează notificarea incidentelor către ANSPDCP, dacă sunt implicate date personale;
- ține evidența prelucrărilor de date în instituție;
- colaborează cu responsabilul IT în caz de incidente.

***Responsabilul GDPR**, în cazul unei scurgeri de date personale, este esențial să cunoască obligațiile legale privind notificarea, inclusiv termenul-limită și autoritățile competente cărora trebuie raportat incidentul.*

Serviciul Resurse umane – responsabilități:

- organizează instruiri periodice pentru angajați pe teme de securitate cibernetică;
- păstrează evidența participării la instruiri;
- informează angajații noi despre regulile de securitate.

***Serviciul Resurse umane** nu face doar angajări, ci și protejează instituția prin instruirea oamenilor.*

Fiecare angajat – responsabilități:

- respectă regulile de securitate (parole, e-mailuri suspecte etc.);
- raportează imediat orice incident sau suspiciune;
- participă la instruirile organizate de instituție;
- nu folosește sisteme ale instituției în scop personal.

6.4. Plan de pregătire continuă și revizuire anuală

De ce este necesar un plan de pregătire continuă? Măsurile de securitate cibernetică implementate trebuie menținute și verificate periodic. Amenințările cibernetice evoluează rapid, iar personalul se poate schimba. Fără pregătire continuă, chiar și cele mai bune măsuri devin ineficiente în timp.

1. Instruirea periodică a personalului:
   - Toți angajații trebuie instruiți cel puțin o dată pe an;
   - Instruirea trebuie să fie adaptată nivelului fiecărui angajat:
     - personal non-tehnic → reguli de bază, phishing, parole;
     - personal tehnic → măsuri avansate, incidente, actualizări tehnice.
   - Trebuie păstrată evidența participării la instruiri.
2. Testarea periodică a măsurilor implementate:
   - Testarea periodică este importantă pentru a verifica dacă:
     - backup-urile funcționează și pot fi restaurate;
     - parolele respectă politica stabilită;
     - angajații recunosc e-mailuri de phishing;
     - sistemele sunt actualizate.
3. Exerciții practice și simulări:
   - Organizarea de simulări de incidente pentru a testa:
     - reacția rapidă a angajaților;
     - procedurile de izolare și raportare;
     - fluxul de comunicare internă și externă.
4. Revizuirea anuală a politicilor și procedurilor:
   - Toate politicile și procedurile de securitate trebuie analizate cel puțin o dată pe an;
   - Trebuie actualizate în funcție de:
     - modificări legislative;
     - recomandările DNSC;
     - incidentele produse în instituție.

Fiecare angajat *este responsabil să raporteze un e-mail suspect, chiar dacă ulterior se dovedește inofensiv. Lipsa raportării poate duce la expunerea instituției la riscuri cibernetice majore.*

Exemplu: primăria X organizează trimestrial sesiuni scurte de instruire despre phishing, cu exemple reale.

Exemplu: în luna martie, primăria a simulat un atac de phishing pentru a vedea câți angajați dau click pe linkuri suspecte.

Exemplu: primăria organizează anual un exercițiu în care se simulează un atac ransomware care blochează calculatoarele.

Exemplu: după un incident de phishing, primăria a revizuit politica de parole și a introdus autentificarea multi-factor.

7. CONCLUZII ȘI RECOMANDĂRI STRATEGICE

Securitatea cibernetică constituie, în actualul context digital, o componentă esențială a funcționării eficiente și responsabile a instituțiilor publice locale. Accelerarea proceselor de digitalizare determină transformarea protecției infrastructurilor informatice și a datelor cu caracter personal dintr-o opțiune tehnică într-un imperativ strategic. Incidentul de securitate cibernetică nu mai reprezintă un scenariu ipotetic, ci o realitate cu impact potențial major asupra continuității operaționale, a serviciilor publice, a reputației instituționale și a încrederii cetățenilor.

Riscurile asociate unui incident cibernetic depășesc considerabil consecințele financiare directe. Efectele pot include întreruperea furnizării serviciilor publice esențiale, expunerea datelor personale, atragerea de sancțiuni legale, degradarea imaginii instituției și chiar apariția unor implicații administrative sau politice semnificative. În acest context, abordarea proactivă a securității cibernetice trebuie să fie tratată ca parte integrantă a bunei guvernanțe locale. Este important de menționat că numeroase măsuri esențiale de securitate nu presupun alocări bugetare semnificative.

Activități precum instruirea periodică a personalului, definirea responsabilităților interne, implementarea de proceduri clare de răspuns la incidente, configurarea corespunzătoare a echipamentelor și utilizarea unor soluții tehnice gratuite sau cu costuri reduse pot contribui semnificativ la reducerea expunerii instituției la amenințări cibernetice. Investițiile în securitatea cibernetică trebuie percepute ca investiții în reziliența organizațională și în continuitatea furnizării serviciilor publice. Acestea contribuie direct la protejarea datelor personale ale cetățenilor, la consolidarea încrederii publice și la creșterea credibilității instituției. O administrație care tratează cu seriozitate protecția infrastructurii sale informatice transmite un semnal clar de responsabilitate și profesionalism.

Succesul în domeniul securității cibernetice nu constă în eliminarea completă a riscurilor, ci în capacitatea instituției de a preveni, detecta, răspunde și recupera eficient în urma unui incident. În acest sens, autoritățile publice locale sunt încurajate să adopte o abordare structurată, bazată pe evaluarea riscurilor, aliniată bunelor practici naționale și europene.

Se recomandă următoarele direcții strategice:

- Integrarea securității cibernetice în strategia de digitalizare a instituției, inclusiv în cadrul proiectelor de tip smart-city, astfel încât dimensiunea securității să fie abordată încă din fazele de planificare și implementare;
- Stabilirea responsabilităților clare privind gestionarea securității cibernetice la nivel instituțional și desemnarea unui punct de contact intern;
- Elaborarea, testarea și actualizarea periodică a planurilor de răspuns la incidente cibernetice, în concordanță cu nivelul de maturitate operațională;
- Organizarea de sesiuni periodice de instruire și conștientizare pentru personal, adaptate rolurilor și nivelului de expunere;
- Prioritizarea investițiilor în funcție de rezultatele evaluărilor de risc, astfel încât resursele disponibile să fie direcționate către domeniile cu cel mai mare impact;
- Consolidarea colaborării cu autoritățile naționale competente, în special cu Directoratul Național de Securitate Cibernetică și cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, pentru asigurarea alinierii la cerințele legale și la standardele în vigoare.

În final, este important ca instituțiile publice locale să trateze securitatea cibernetică nu doar ca o obligație de conformare, ci ca pe un factor determinant al modernizării și eficienței administrative. Transformarea digitală sustenabilă este posibilă doar în condițiile în care infrastructura informatică este protejată adecvat, iar funcționarii publici sunt pregătiți să acționeze eficient în fața amenințărilor cibernetice.[11]

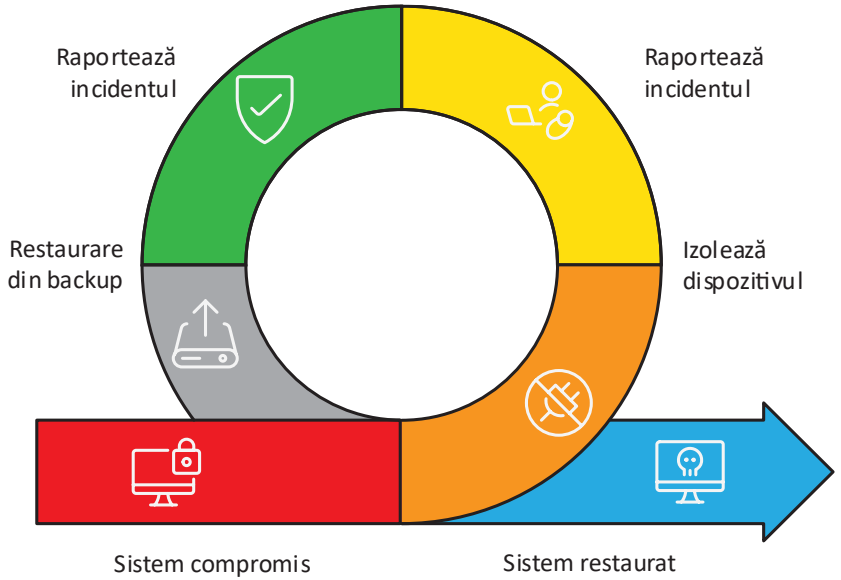
ANEXA 1 – CHECKLIST DE SECURITATE CIBERNETICĂ

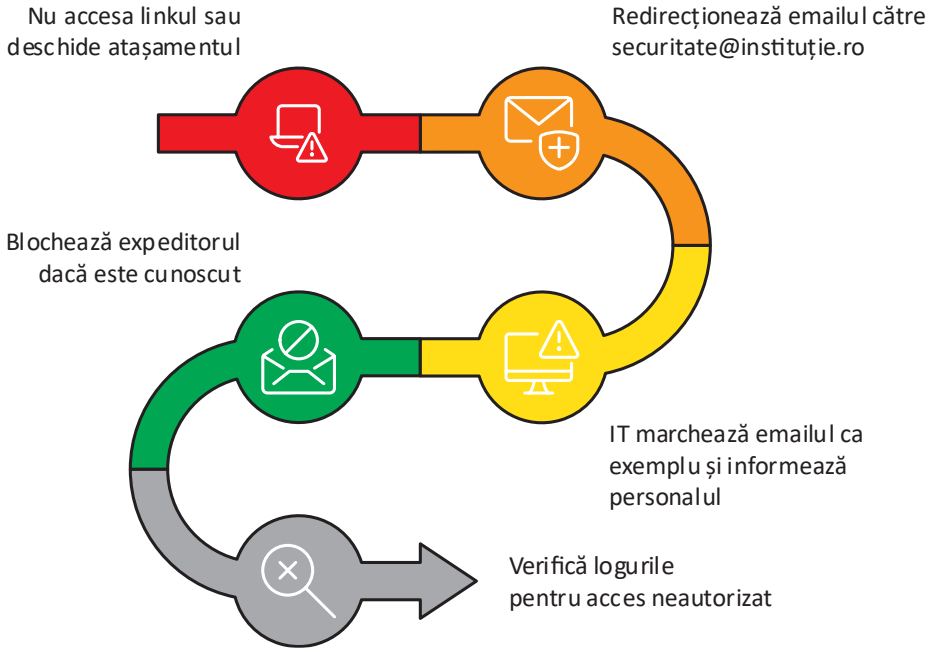
Nr.	Măsură de verificat	Da	Nu	Observații
1	Parolele conturilor de utilizator au fost schimbate în ultimele 6 luni	☐	☐	
2	Autentificarea multifactor (MFA) este activă pentru e-mail și conturi cloud	☐	☐	
3	Antivirusul este instalat și activ pe toate stațiile de lucru	☐	☐	
4	Actualizările de securitate Windows sunt aplicate	☐	☐	
5	Backup-urile se efectuează conform regulii 3-2-1 și au fost testate recent	☐	☐	
6	Dispozitivele USB sunt controlate și scanate automat	☐	☐	
7	Rețelele Wi-Fi (publice și interne) sunt protejate prin parolă și criptare WPA2/3	☐	☐	
8	Există o listă actualizată de utilizatori activi și permisiunile sunt verificate	☐	☐	
9	Accesul la date sensibile este restricționat în funcție de rol	☐	☐	
10	Politicile interne de securitate au fost comunicate personalului	☐	☐	
11	Cel puțin o sesiune de instruire în domeniul igienei cibernetice a fost realizată	☐	☐	
12	Planul de răspuns la incidente este cunoscut de persoanele desemnate	☐	☐	
13	S-au verificat log-urile de activitate ale serverelor sau stațiilor critice	☐	☐	
14	S-au identificat conturi necunoscute sau activitate suspectă	☐	☐	
15	Procedurile de raportare sunt afișate vizibil (intranet/panou)	☐	☐	

Data verificării: _____

Responsabil verificare: _____

ANEXA 2 - PROCEDURI PAS-CU-PAS PENTRU SITUAȚII DE CRIZĂ





Atac ransomware - pași de urmat:

1. nu opri calculatorul, pentru a nu pierde informații utile investigației;
2. deconectează dispozitivul de la rețea (Wi-Fi sau cablu) pentru a opri propagarea atacului;
3. informează imediat IT-ul și conducerea instituției;
4. raportează incidentul în platforma PNRISC către DNSC;
5. nu plăti răscumpărarea. Restaurarea se face doar din backup valid.

E-mail suspect - măsuri rapide:

1. nu deschide linkuri sau atașamente necunoscute;
2. trimite e-mailul suspect către adresa oficială de securitate (ex. *securitate@instituție.ro*);
3. blocarea expeditorului se face dacă este o adresă deja recunoscută ca malițioasă;
4. e-mailul este marcat ca exemplu pentru conștientizare;
5. log-urile sunt verificate pentru a detecta acces neautorizat.

ANEXA 3 – LISTA DE CONTACTE UTILE

AUTORITĂȚI NAȚIONALE

Instituție	Contact		Rol
DNSC – Directoratul Național de Securitate Cibernetică	*pnrisc.dnsc.ro*	**1911**	Notificare incidente
ANSPDCP – Protecția Datelor	*contact@dataprotection.ro*	**0318 059 211**	Notificare breșe de date

FURNIZORI TEHNICI (EXEMPLE)

Serviciu	Contact	
Sistem de operare și pachet aplicații pentru productivitate	*adresă oficială de e-mail companie*	*număr oficial companie*
Platformă de colaborare și stocare online	*adresă oficială de e-mail companie*	*număr oficial companie*
Soluție de securitate cibernetică – antivirus și protecție endpoint	*adresă oficială de e-mail companie*	*număr oficial companie*
Serviciu de backup și recuperare date în cloud	*adresă oficială de e-mail companie*	*număr oficial companie*

CONTACTE INTERNE

Responsabil	Nume	Telefon	Email
Responsabil IT	*nume si prenume responsabil*	*număr de telefon*	*adresă de email*
DPO (protecția datelor)			
Purtător de cuvânt			

Actualizează trimestrial acest tabel cu informațiile corecte.

ANEXA 4 - STUDIU DE CAZ - PRIMĂRIA SECTOR 5 BUCUREȘTI

Contextul incidentului: la 26 octombrie 2024, sistemele informatice ale Primăriei Sectorului 5 București au fost grav afectate de un atac ransomware, care a blocat activitatea instituției. Pe servere a fost afișat un mesaj prin care atacatorii solicitau plata unei răscumpărări de 5 milioane USD pentru decriptarea datelor compromise. Gruparea infracțională RansomHub[12] a revendicat atacul, fiind cunoscută pentru activitatea sa internațională.

Impactul atacului: potrivit informațiilor publice, aproximativ 200.000 de persoane au fost afectate. Date personale sensibile - precum nume, CNP-uri, adrese și alte informații - au fost sustrase și conform surselor, scoase la vânzare pe Dark Web. Activitatea instituției a fost sever perturbată: bazele de date și sistemele informatice au devenit inaccesibile, iar canalele de comunicare au fost întrerupte. Refacerea infrastructurii IT a necesitat intervenții urgente și costuri semnificative.

Acțiunile Primăriei Sectorului 5: instituția a notificat imediat autoritățile competente, inclusiv DNSC, și a refuzat plata răscumpărării, optând pentru restaurarea datelor din copii de siguranță. A fost demarată o anchetă internă și s-a colaborat cu structurile abilitate, cu angajamentul de a consolida măsurile de securitate cibernetică.

Intervenția și poziția DNSC: Conform răspunsului oficial transmis către „Buletin de București", DNSC a fost notificat în aceeași zi în care incidentul a fost identificat, raportarea oficială fiind transmisă prin platforma PNRISC pe 31 octombrie 2024. O echipă de intervenție rapidă s-a deplasat la fața locului, oferind suport tehnic și asistență pentru investigarea incidentului și limitarea impactului. DNSC a recomandat deconectarea imediată a infrastructurii IT&C de la rețea, conservarea probelor digitale și implementarea măsurilor de remediere. Directoratul a subliniat că nu a fost implicat în eventuale negocieri cu atacatorii, reiterând poziția oficială conform căreia plata răscumpărărilor este ferm descurajată. De asemenea, cetățenilor ale căror date ar fi putut fi compromise li se recomandă schimbarea parolelor, activarea autentificării în doi pași și raportarea tentativelor de fraudă la numărul 1911.

Recomandări DNSC: În ceea ce privește măsurile de prevenție, DNSC a recomandat:

- realizarea periodică a copiilor de siguranță;
- instalarea de soluții antivirus actualizate;
- segmentarea rețelei;
- utilizarea firewall-urilor moderne și a parolelor complexe;
- evitarea utilizării necontrolate a aplicațiilor de acces de la distanță.

Referințe web: [13, 14, 15]

ANEXA 5 - GLOSAR DE TERMENI ȘI ACRONIME

Termen	Definiție
Active Directory (AD)	Serviciu Microsoft care stochează informații despre obiecte din rețea și le pune la dispoziția utilizatorilor și administratorilor
Antivirus	Software care detectează, previne și elimină programe malițioase de pe calculator
Application Programming Interface (API)	Set de protocoale și instrumente pentru construirea aplicațiilor software
Backup	Copie de rezervă a datelor pentru recuperarea lor în caz de pierdere sau deteriorare
Baiting	Tehnică de inginerie socială care folosește „momeala” pentru a compromite securitatea
BitLocker	Funcție de criptare a discurilor disponibilă în Windows
Bring Your Own Device (BYOD)	Politica care permite angajaților să folosească dispozitivele personale la locul de muncă
Business Email Compromise (BEC)	Tip de atacuri cibernetice care vizează companiile prin compromiterea email-urilor de afaceri
Cloud computing	Furnizarea de servicii de calculator prin internet
Credential stuffing	Atac cibernetic care folosește perechi de nume de utilizator și parole compromise
Criptare	Procesul de transformare a informațiilor într-un format neinteligibil pentru a le proteja
Cross-site Request Forgery (CSRF)	Tip de atac malițios care exploatează încrederea unui site web în browser-ul utilizatorului
Cross-site Scripting (XSS)	Vulnerabilitate care permite atacatorilor să injecteze scripturi malițioase în pagini web
Deepfake	Tehnologie IA care creează conținut video sau audio fals, dar realist
Domain Name System (DNS)	Sistem care traduce numele de domenii în adrese IP
Double extortion	Tactică de ransomware care implică atât criptarea datelor, cât și amenințarea cu publicarea lor
Endpoint	Orice dispozitiv conectat la rețea (calculator, telefon, tabletă)
Evil twin	Punct de acces Wi-Fi fals creat pentru a fura informații
Firewall	Sistem de securitate care monitorizează și controlează traficul de rețea
Firmware	Software de nivel scăzut care controlează componentele hardware

Termen	Definiție
GDPR	Regulamentul european privind protecția datelor
Hash	Funcție matematică care transformă datele în șiruri de caractere de lungime fixă
HTTPS	Protocol securizat pentru transferul de date pe web
Inginerie socială	Manipularea psihologică a oamenilor pentru a dezvălui informații confidențiale
Internet of Things (IoT)	Rețeaua de obiecte fizice conectate la internet
Jurnal (Log)	Înregistrare automată a evenimentelor dintr-un sistem informatic
Living-off-the-land attacks	Atacuri care folosesc instrumente legitime ale sistemului pentru activități malițioase
Macro	Secvență de instrucțiuni automatizate în aplicații precum Microsoft Office
Malware	Software malițios conceput să dăuneze sau să compromită sisteme informatice
Mobile Device Management (MDM)	Gestionarea centralizată a dispozitivelor mobile
Multi-Factor Authentication (MFA)	Autentificare care necesită două sau mai multe metode de verificare
OneDrive	Serviciu de stocare în cloud oferit de Microsoft
Password spraying	Atac care încearcă parole comune pe mai multe conturi
Patch	Actualizare software pentru corectarea vulnerabilităților
Patch management	Procesul de gestionare a actualizărilor de securitate
Phishing	Încercare de obținere a informațiilor sensibile prin înșelăciune
PNRISC	Platforma Națională de Raportare a Incidentelor de Securitate Cibernetică
PowerShell	Interpretor de comenzi și limbaj de scripting Microsoft
Pretexting	Tehnică de inginerie socială bazată pe scenarii false
Quid pro quo	Tehnică de inginerie socială bazată pe oferirea de servicii în schimbul informațiilor
Ransomware	Tip de malware care blochează accesul la date și cere plată pentru deblocare
Remote Desktop Protocol (RDP)	Protocol pentru accesul de la distanță la calculatoare

Termen	Definiție
SIM swapping	Furtul identității prin transferul numărului de telefon pe o cartelă SIM diferită
Single Sign-On (SSO)	Sistem care permite autentificarea cu un singur set de credențiale
Smishing	Phishing prin SMS
SQL injection	Atac care exploatează vulnerabilități în bazele de date
Supply chain	Lanțul de aprovizionare, în context cibernetic se referă la atacuri prin furnizori
Tailgating	Urmărirea neautorizată a unei persoane autorizate pentru a obține acces
Token	Element de securitate folosit pentru autentificare
Two-factor authentication (2FA)	Autentificare în doi pași
Universal Serial Bus (USB)	Interfață pentru conectarea dispozitivelor
Virtual Local Area Network (VLAN)	Rețea locală virtuală
Virtual Private Network (VPN)	Rețea privată virtuală pentru conexiuni securizate
Whaling	Tip de phishing care vizează persoane importante din organizații
Wi-Fi	Tehnologie de rețea wireless
Windows Management Instrumentation (WMI)	Tehnologie Microsoft pentru gestionarea sistemelor
Wiperware	Malware destinat distrugerii ireversibile a datelor
WPA2/WPA3	Protocoale de securitate pentru rețele wireless
Zero-day	Vulnerabilitate necunoscută public și neacoperită de patch-uri

NOTE DE FINAL

[1] https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf
[2] https://www.enisa.europa.eu/sites/default/files/publications/ETL2020%20-%20Phishing%20A4.pdf
[3] https://news.sophos.com/en-us/2024/08/14/the-state-of-ransomware-in-state-and-local-government-2024/
[4] https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024
[5] https://www.dnsc.ro/vezi/document/ghid-protectie-functionari-publici
[6] https://www.dnsc.ro/vezi/document/dnsc-ghid-inginerie-sociala
[7] https://www.honeywell.com/us/en/press/2024/04/honeywell-report-reveals-silent-residency-is-driving-escalating-cyber-threat-for-industrial-and-critical-infrastructure-facilities
[8] https://www.cisa.gov/about/2024YIR
[9] https://owasp.org/Top10/
[10] https://rublon.com/uncategorized/nis2-mfa-requirements-enisa-guidance
[11] https://legislatie.just.ro/Public/DetaliiDocument/250235
[12] https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-ransomhub
[13] https://buletin.de/bucuresti/wp-content/uploads/Raspunsul-DNSC-pentru-Buletin-de-Bucuresti.pdf
[14] https://www.digi24.ro/stiri/actualitate/evenimente/serverele-primariei-sector-5-atacate-de-hackeri-care-cer-o-rasumparare-de-5-milioane-de-dolari-2983405#
[15] https://buletin.de/bucuresti/datele-furate-de-la-primaria-sectorului-5

Exemplele și scenariile de atac prezentate în acest ghid sunt inspirate din cazuri reale și vulnerabilități identificate în mediul digital. Cu toate acestea, ele au un caracter generic și au fost create cu scopul de a ilustra amenințările și măsurile de protecție într-o manieră cât mai accesibilă. Aceste exemple nu fac referire la o anumită primărie sau instituție publică. Orice similitudine cu evenimente sau entități concrete este pur întâmplătoare și servește exclusiv scopului didactic al ghidului.

Autori: Daniel Abotezătoaei, Cristian Nistor, Ciprian Savu

TLP:CLEAR se poate folosi atunci când informațiile prezintă un risc minim sau inexistent de utilizare necorespunzătoare, în conformitate cu normele și procedurile aplicabile pentru publicarea informațiilor. Destinatarii pot partaja aceste informații fără restricții. Informațiile fac obiectul normelor standard privind drepturile de autor.

https://www.dnsc.ro/