
IESP
INSTITUTUL EUROPEAN DE STUDII POLITICE
Kingdom of the Netherlands
UK Government
INSTITUTE FOR WAR & PEACE REPORTING
IWPR
EU-Moldova
Stronger Together
eGA
WOMEN
IN CYBER
www.womenincyber.md

Acțiunile și evenimentele programului de mentorat "WOMEN IN CYBER" au fost realizate și organizate în cadrul proiectului "Femeile în domeniul securității și menținerii păcii: construirea diversității, accesibilității și echipelor mai puternice", finanțat printr-un grant al Institutului pentru Raportare despre Război și Pace (IWPR) cu suportul Guvernului Regatului Unit al Marii Britanii și Irlandei de Nord.

Opiniile, constatările și concluziile menționate aparțin autorilor și nu reflectă neapărat viziunea IWPR și Guvernului Britanic.

www.womenincyber.md

Cuprins

Cuvânt de salut

Natalia SPÎNU
Director, Institutul European de Studii Politice din Moldova

Frecvența și diversificarea atacurilor cibernetice atât pentru utilizatori cât și pentru organizații, au încurajat peste 200 de doamne și domnișoare să se înscrie online (womenincyber.md) la instruirile, atelierele de lucru, evenimentele, conferințele din domeniul securității cibernetice desfășurate în cadrul Programului de mentorat "WOMEN IN CYBER".

Programul a durat cinci luni și a avut ca scop încurajarea dezvoltării abilităților femeilor și fetelor din Republica Moldova în domeniul securității cibernetice prin instruire, schimb de experiență, conferințe motivaționale între mentore și participante.

În prezent, domeniul securității cibernetice atrage tot mai multe tinere. Este o șansă enormă pentru a schimba ceva și mă bucur să văd că din ce în ce mai multe femei aleg să își înceapă o carieră în securitatea cibernetică, indiferent că sunt proaspăt absolvente sau că aleg să își schimbe cariera.

Institutul European de Studii Politice din Moldova (IESPM) contribuie activ pentru a crește gradul de diversitate din domeniu, susținând femeile ambițioase prin programe de mentorat precum"WOMEN IN CYBER", prin informații esențiale care să le ajute să facă față provocărilor profesionale și prin acces la comunitatea infosec atât din Republica Moldova, cât și din plan internațional.

Cursurile din domeniu care s-au desfășurat în cadrul programului au oferit o sistematizare eficientă a conceptelor teoretice și un grad ridicat de abilitate practică.

Personalul calificat este foarte important în acest domeniu și de aceea IESPM pune accent pe colaborările cu universitățile din Republica Moldova, organizații neguvernamentale și pregătim noile generații prin programe de training și internship.

Traiectoria profesională a femeilor în domeniu a fost un subiect central și va continua să fie o prioritate pentru profesioniștii din industrie.Liderii infosec recunosc și susțin importanța diversității și potențialul extraordinar al femeilor în domeniul securității cibernetice, de la nivelul de executor și până la cele de conducere.

Unul dintre motivele principale pentru a alege o carieră în acest domeniu este

cererea crescută de profesioniști. Atacurile cibernetice au crescut exponențial în ultimii ani, determinând companiile să investească masiv în protejarea datelor și infrastructurii lor. Acest lucru a condus la o cerere masivă de specialiști în securitate cibernetică, un trend care se pare că nu va încetini prea curând. Conform rapoartelor, în 2022 existau peste 3 milioane de posturi vacante în domeniul securității cibernetice la nivel global, semn că este un domeniu în plină expansiune.

În plus, alegerea unei cariere în securitatea cibernetică poate aduce satisfacții financiare considerabile. Specialiștii în securitate cibernetică sunt remunerați generos, reflectând atât cererea mare, cât și nivelul de expertiză necesar. Salariile competitive sunt o dovadă a valorii pe care societatea o atribuie acestui domeniu și a importanței muncii pe care acești profesioniști o fac.

Dar securitatea cibernetică nu este doar despre salarii atractive și o cerere mare de forță de muncă. Este un domeniu care oferă o provocare intelectuală semnificativă. Amenințările cibernetice evoluează constant, iar specialiștii în securitate cibernetică trebuie să fie mereu cu un pas înaintea infractorilor. Aceasta presupune o învățare continuă, creativitate și gândire strategică, făcând cariera în securitatea cibernetică una extrem de dinamică și stimulativă.

În fine, o carieră în securitatea cibernetică oferă oportunitatea de a avea un impact pozitiv semnificativ. În calitate de specialist în securitate cibernetică, munca ta va contribui la protejarea datelor personale, financiare și critice ale oamenilor și organizațiilor. Aceasta nu este doar o responsabilitate mare, ci și o onoare, deoarece rolul tău poate ajuta la construirea unei lumi digitale mai sigure.

Fâcând o retrospectivă la cele menționate anterior, sunt recunoscătoare Institutului pentru Raportare despre Război și Pace (IWPR) și Guvernului Regatului Unit al Marii Britanii și Irlandei de Nord pentru lansarea unui program de mentorat în domeniul securității cibernetice în Republica Moldova, precum și pentru tot suportul oferit de către Guvernul Regatului Țărilor de Jos și Academia de e-Guvernare din Estonia întru desfășurarea și organizarea atelierilor de lucru și a cursurilor de instruire în domeniul securității cibernetice.

Sunt încrezătoare că această inițiativă va sprijini câteva parteneriate excelente, și ne va ajuta să evidențiem modele de inspirație feminină care vor încuraja multe alte femei și fete să se alăture acestui domeniu cu o creștere rapidă.

Vă mulțumesc și mult succes tuturor!

Cuvânt de salut

Epp MAATEN - Team Leader, Proiectul UE de Asistență rapidă pentru securitatea cibernetică în Republica Moldova, implementat de Academia de e-Guvernare din Estonia

Securitatea cibernetică a devenit o parte esențială a politicilor și strategiilor guvernamentale de securitate. De ce? Pe măsură ce guvernele încep să construiască o societate informațională, acestea se concentrează, de obicei, pe furnizarea de servicii digitale. Securitatea cibernetică a societății va primi o atenție sporită doar atunci când aceste servicii nu vor fi brusc disponibile sau când datele vor fi incorecte. Cu alte cuvinte - securitatea cibernetică devine adesea importantă doar după un incident de securitate de amploare sau dăunător.

În același timp, securitatea cibernetică este o parte integrantă a unei societăți informaționale. Serviciile electronice, cum ar fi e-banking-ul sau e-administrarea taxelor, nu au niciun rost dacă funcționarea lor și confidențialitatea datelor transmise sunt puse sub semnul întrebării. Securitatea ar trebui să fie întotdeauna parte integrantă a e-guvernării și a societății în general - considerațiile de securitate trebuie să fie incluse în fiecare serviciu electronic, cum ar fi portalul de stat, semnătura digitală și așa mai departe.

Cu toate acestea, avem nevoie și de o anumită alfabetizare tehnologică la nivel individual, de care avem nevoie cu toții dacă dorim nu numai să funcționăm într-o societate digitalizată, ci și să ne asigurăm că nu creăm riscuri pentru aceasta prin comportamentul nostru. Înțelegerea riscului cibernetic pentru societatea digitală este esențială pentru a determina rezistența acesteia. Programul de mentorat "WOMEN IN CYBER", implementat împreună cu Institutul European de Studii Politice din Moldova și cu Institutul pentru Raportare despre Război și Pace (IWPR) cu suportul Guvernului Regatului Unit al Marii Britanii și Irlandei de Nord, a avut drept scop să aducă dialog, discuții și conversații deschise cu privire la cibernetică ca subiect și, de asemenea, să înțeleagă mai bine aspectele securității cibernetice. Numeroase ateliere de lucru au oferit sfaturi practice cu privire la măsurile de protecție de bază pe care toată lumea ar trebui să le urmeze în spațiul cibernetic pentru a asigura securitatea tranzacțiilor digitale atunci când lucrează la distanță, precum și pentru a înțelege conceptele de bază din spatele atacurilor de inginerie socială. Programul a fost conceput pentru a sprijini egalitatea de gen, emanciparea femeilor și a fetelor.

Despre proiect

Dezvoltarea societăților digitale este în centrul atenției aproape peste tot în lume. Cu toate acestea, securitatea instrumentelor și sistemelor digitale este adesea neglijată, deoarece este complexă și poate fi costisitoare din cauza lipsei de cunoștințe. Acest lucru a condus la necesitatea de a defini la nivel național capacitățile de securitate cibernetică de care are nevoie fiecare societate digitală.

Există mai multe standarde și orientări internaționale pentru dezvoltarea securității cibernetice a unei singure organizații, dar este o sarcină complicată să se găsească instrumente cuprinzătoare și universale pentru guvernele naționale. În primăvara anului 2022, Uniunea Europeană a inițiat Proiectul de asistență rapidă în domeniul securității cibernetice în Moldova. Scopul proiectului este de a spori reziliența cibernetică a organizațiilor din sectorul public și a sectoarelor cheie de infrastructură critică. Academia de e-Guvernare din Estonia este organizația de implementare a proiectului. Obiectivul asistenței rapide este de a contribui la cadrul de reglementare și la capacitatea instituțională a Republicii Moldova în ceea ce privește securitatea rețelelor și a informațiilor, precum și de a spori reziliența cibernetică a organizațiilor din sectorul public și a sectoarelor cheie de infrastructură critică din Moldova. În acest cadru, sarcinile-cheie sunt stabilirea unui model funcțional de guvernanță pentru securitatea cibernetică și protecția infrastructurii critice, precum și ajustarea cadrului normativ privind securitatea cibernetică.

În plus, proiectul vizează consolidarea capacităților părților interesate din Republica Moldova, permite elaborarea cadrelor juridice ale instituțiilor din domeniul securității cibernetice și alinierea acestora la strategia, standardele și cadrul juridic și politic relevant al UE, în special la Directiva UE privind securitatea rețelelor și a informațiilor.

Academia de e-Guvernare dorește să mulțumească Nataliei Spînu și echipei sale de la Institutul European de Studii Politice din Moldova pentru angajamentul lor și pentru implementarea cu succes a programului de mentorat "WOMEN IN CYBER".

Cuvânt de salut

Olesea GARBUZ

Ofițer de proiect, Institutul pentru Raportare despre Război și Pace (IWPR)

În cadrul proiectului BREN, cu scopul de a consolida reziliența societății civile în țările din vecinătatea estică, Institutul pentru Raportare despre Război și Pace (IWPR) s-a focusat mult pe rolul femeii în promovarea păcii, securității și stabilității. Motto – ul Institutului pentru Raportare despre Război și Pace este "Giving Voice, Driving Change" – să oferi voce și să determine schimbare. Experiența IWPR se bazează pe susținerea vocilor excluse, iar acestea de cele mai dese ori sunt femei, acele voci care sunt deseori excluse din procesul de luare a deciziilor.

Cuvântul cheie în cadrul proiectului nostru este "reziliența", pentru că toate activitățile implementate de cei 11 parteneri din cadrul proiectului BREN, sunt îndreptate spre consolidarea rezilienței organizațiilor sau a comunității în fața pericolelor care determină coflictele, instabilitatea și insecuritatea.

Am urmărit cu mare interes tematica sesiunilor la care au participat beneficiarele programului "Women in Cyber"și consider că a fost o oportunitate excelentă pentru să cunoască mai multe despre cum o femeie își poate crește rolul în domeniul securității cibernetice și cât de important este implicarea femeilor în acest domeniu.

Programul de mentorat "Women in Cyber" a fost menit să motiveze și să încurajeze participantele să beneficieze de cunoștințele și experiența acumulată, care ar putea să le ghideze la locul de muncă, în viața cotidiană sau într-un nou domeniu, cum ar fi securitatea cibernetică. Ne dorim mult ca vocile femeilor participante la programul de mentorat să se facă auzite, iar cunoștințele obținute aici să fie utile. Sper că participantele vor deveni multiplicatori și persoane-resursă capabile să transmită cunoștințele și experiența acumulată celor interesați. Dar cel mai important cred, este să păstreze comunitatea de femei creată, prima promoție de Women in Cyber, să se promoveze reciproc și să promoveze rolul femeii în acest domeniu în afara comunității.

Femeile în domeniul securității și menținerii păcii: construirea diversității, accesibilității și echipelor mai puternice

Institutul European de Studii Politice din Moldova (IESPM), în perioada octombrie 2022 – martie 2023 a implementat programul de mentorat "WOMEN IN CYBER", o inițiativă dedicată promovării, susținerii și afirmării femeilor în domeniul securității cibernetice.

Scopul programului este să încurajeze dezvoltarea abilităților femeilor și fetelor din Republica Moldova în domeniul securității cibernetice prin instruire, schimb de experiență, conferințe motivaționale între mentori și participante.

Mentorii IESPM și experții din domeniu au oferit sprijin participantelor pentru a beneficia de suport și asistență în procesul de consiliere în formarea unei cariere de succes în domeniul securității cibernetice, de la alegerea unei facultăți de profil și obținerea certificatelor la cursurile absolvite, regulile de urmat pentru elaborarea unui portofoliu profesional și a unui CV calitativ, până la posibilitatea de angajare la un loc de muncă potrivit aptitudinilor lor.

Importanța mentorilor din cadrul programului "WOMEN IN CYBER" - joacă un rol esențial în creșterea profesională a participantelor.Mai mult decât atât, pe parcursul acestor luni productive, participantele au cunoscut și au făcut schimb de informații cu persoane notorii din acest domeniu.

Prin urmare, programul de mentorat a reușit să asigure instruiri în domeniul securității cibernetice să inspire și să motiveze participantele prin propriile exemple, cunoașteri, îndrumându-le spre o carieră de succes; să asigure colaborare cu alte mentore pentru a crea un schimb de experiență de lungă durată; definească obiective clare; să promoveze egalitatea de gen în sectorul securității cibernetice.

PROGRAMUL DE MENTORAT

WOMEN IN CYBER

Instruiri și conferințe motivaționale în domeniul securității cibernetice

Conferința Internațională „Femeile în spațiul cibernetic: importanța incluziunii în strategia de securitate regională și în Moldova”

Incluziunea femeilor în domeniul securității cibernetice ar putea contribui la îmbunătățirea strategiilor de țară, dar și să facă națiunile mai reziliente în fața acestor provocări. Subiectul a fost discutat pe larg la conferința internațională „Femeile în spațiul cibernetic: importanța incluziunii în strategia de securitate regională și în Moldova”, desfășurată în premieră la Chișinău, pe data de 17 decembrie 2022.

Evenimentul a cuprins câteva paneluri de discuții cu privire la schimbările dinamice în contextul geopolitic și modalități de a găsi soluții pentru problemele emergente, dar și construirea următoarei generații de lideri cibernetici.

De asemenea, conferința a avut drept scop reiterarea importanței incluziunii femeilor în domeniul securității cibernetice, așa cum și nevoia unui număr mai mare de profesioniști se află în ascensiune, în contextul atacurilor cibernetice în creștere.

Evenimentul s-a desfășurat în incinta Centrului de Excelență în IT „Tekwill” și a adunat peste 80 de participanți interesați să cunoască opiniile invitaților: experți naționali și internaționali din Uniunea Europeană, Statele Unite ale Americii, Singapore, Regatul Unit al Marii Britanii, Moldova și alte state.

Natalia SPÎNU, Director al Institutului European de Studii Politice din Moldova (IESPM): "Această conferință va sprijini câteva parteneriate excelente și va ajuta la evidențierea modelelor de inspirație feminină, care vor încuraja multe alte femei și fete să se alăture acestui domeniu aflat în plină ascensiune. Cercetările arată că o diversitate mai mare în echipe oferă rezultate mai mari, iar securitatea cibernetică nu valorifică actualmente un imens fond de talente și potențial - femeile. În plus, ar trebui create roluri manageriale de securitate cibernetică pentru femei, să poată alege o carieră în domeniul securității cibernetice. Încurajarea femeilor și fetelor să joace un rol activ în sectorul digital este importantă, deoarece egalitatea de șanse se află chiar în centrul unei societăți cu adevărat egale în care toată lumea poate prospera și își poate realiza întregul potențial."

Conferința a fost onorată și de prezența: Excelenței Sale, **Steven FISHER**, Ambasadorul Extraordinar și Plenipotențiar al Regatului Unit al Marii Britanii și Irlandei de Nord în Republica Moldova; **Anthony BORDEN**, Director Executiv al Institutului pentru Raportare despre Război și Pace, **Stella JEMNA**, Șefă de Cabinet a Prim-ministrei Republicii Moldova;

Dominika STOJANOSKA, Reprezentantă de țară UN Women în Republica Moldova; **Ana CHIRIȚA**, Directoarea Proiectelor Strategice al Asociației Naționale al Companiilor ICT, Director de Proiect Tekwill; **Joanneke BALFOORT**, Director Politica de Securitate și Apărare, Serviciul European de Acțiune Externă, Bruxelles; **Viorel CIBOTARU**, Ambasadorul Extraordinar și Plenepotențiar al Republicii Moldova în Regatul Belgiei și Marele Ducat al Luxemburgului. Șeful Misiunii Republicii Moldova la NATO; **Julie LIMAGES**, ofițer economic la Ambasada SUA în Republica Moldova; **Christiane WUILLAMIE OBE FIRL**, Inovație, Risc și Performanță pentru consolidarea Culturii de Securitate Cibernetică și Managementul Tehnologiilor (Londra, Marea Britanie); **Luigi REBUFFI**, Secretar General la Organizația Europeană de Securitate Cibernetică (ECSO) și Women4Cyber (W4C), Bruxelles; **Poogia SHIMPI**, Ofițer de Securitate Informațională a Bussines-ului, Citi Bank (Singapore); **Klaudia GEBALA**, Arhitectă Soluție Cloud, Securitate, Identitate și Conformitate, Microsoft (Polonia); **Elena MÂRZAC**, experta StratCom, Co-fondatoare&Directoare StratCom și Colaborarea Internațională, PISA; **Diana MOLODILOV**, expertă în leadership militar feminin la Universitatea Massachusetts; **Cristina SCHIMBOV**, Președinta Asociației Femeilor din Poliție; **Gabriela RADU**, expertă în securitate cibernetică (România).

Printre cele mai importante informații de la panelurile de discuții s-au regăsit:

1. Republica Moldova urmează o serie de pași pentru îmbunătățirea securității pe mai multe domenii, unul dintre acestea fiind cel al securității cibernetice. În ultima perioadă, au fost înregistrate mai multe atacuri cibernetice atât la nivelul sectorului privat, cât și a celui public. Ambasada Regatului Unit al Marii Britanii și Irlandei de Nord cu autoritățile țării în vederea perfecționării și dezvoltării securității cibernetice.
2. Securitatea cibernetică a devenit o prioritate pentru tot mai multe țări. În prezent, tot mai multe state își regândesc strategiile naționale, în perspectiva consolidării rezilienței la amenințările cibernetice.
3. Un rol important îi revine diplomației cibernetice, care contribuie la prevenirea conflictelor, atenuarea amenințărilor la adresa securității cibernetice și la o mai mare stabilitate în relațiile internaționale. Iar, consolidarea rezilienței în Europa de Est.

Modulul I. Ingineria socială

În perioada 12-14 decembrie 2022 a fost organizat primul training în cadrul programului de mentorat "WOMEN IN CYBER" – Inginerie socială.

Participantele au avut onoarea de a-l avea în calitate de trainer pe domnul **Andy Humphrys**, expert în securitate cibernetică al Academiei de e-Guvernare din Estonia.

Pe parcursul a trei zile au fost explicate și analizate atât prin intermediul lecțiilor teoretice, dar și exercițiilor practice fundamentele ingineriei sociale, cadrul general, vectorii de atac (vishing, phishing, smishing, imposture etc.), modalitățile de obținere a informațiilor, profilul comportamental, psihologia, metodologia și aspectele legale ale ingineriei sociale. Participantele au învățat cum să gestioneze unele dintre provocările etice și de risc asociate angajamentelor de inginerie socială, devenită o necesitate vitală în contextul amplificării amenințărilor venite din spațiul cibernetic.

Modulul II. Asigurarea securității pe dispozitivele mobile

Atacurile cibernetice sunt în continuă creștere la nivel global, iar prevenția lor reprezintă una dintre cele mai sustenabile soluții, în special în domeniul telecomunicațiilor.Studiile internaționale arată că, numai în 2022, aproape fiecare a 2-a companie declară că a suferit o încălcare de securitate în care a fost implicat anume un dispozitiv mobil. Iată de ce, companiile din domeniu depun eforturi pentru a își îmbunătăți capacitățile de răspuns și a asigura reziliența infrastructurii digitale, a rețelelor și a serviciilor.

Subiectul a fost discutat în cadrul training-ului organizat în data de 16 decembrie 2022 de către Institutul European de Studii Politice din Moldova în parteneriat cu Orange Moldova.Printre invitații evenimentului s-au regăsit și experți internaționali.

Natalia SPÎNU, Director, Institutul European de Studii Politice din Moldova (IESPM): *„Securitatea dispozitivelor mobile este strategia, infrastructura și software-ul folosit pentru a proteja orice dispozitiv al utilizatorilor, precum smartphone-uri, tablete și laptopuri. Iar cum dispozitivele mobile sunt din ce în ce mai mult integrate în viața zilnică, gestionarea riscului pentru sistemele informatice este fundamentală pentru asigurarea unei securități eficiente. Scopul workshop-ului a fost de a familiariza participanții și de a le spori capacitățile în domeniul securității cibernetice în general și al securității dispozitivelor mobile în mod particular, obiectiv pe care ni l-am propus prin acest parteneriat cu Orange Moldova. Astfel, punem în evidență provocările legate de securitatea cibernetică, facem schimb de bune practici și încurajăm cooperarea între profesioniștii din domeniu."*

Printre temele de discuție la eveniment, s-au numărat probleme de actualitate cu privire la vulnerabilitățile sistemelor informatice și amenințările care pot dăuna securității mobile: fizice, aplicațiile, de rețea, bazate pe web și endpoint. De asemenea, au fost abordate și aspecte care vizează componentele securității mobile - scanere de penetrare, VPN, auditul și controlul dispozitivului, securitatea contului de e-mail etc.

Dispozitivele mobile, mai vulnerabile la atacurile virtuale

Dispozitivele mobile au o suprafață de atac mult mai mare, fiind o amenințare mai semnificativă pentru securitatea corporativă, ele sunt cele mai vulnerabile la atacuri fizice și virtuale.

Gul ALTUNG, expertă în securitate cibernetică la Ministerul Apărării al Olandei: *„Un telefon mobil are aceeași intrare în datele noastre, dar în general poate fi mai puțin sigur decât un computer. Am explicat acest subiect, întrucât este cu adevărat important și am împărțit această discuție în două componente principale, criminalistică și ofensivă. Iată de ce, reiterez importanța cunoștințelor despre anatomia unei securități mobile."*

Securitatea este o cultură și nu o prescripție IT

Pentru o dezvoltare durabilă a unei companii și o abordare corporativă de responsabilitate socială, domeniul de securitate trebuie să fie privit global, odată ce din cauza amenințărilor în schimbare, complexității şi eterogenității lor, nu mai este posibil să se ia în considerare diferite aspecte ale securității independent una de cealaltă. Ridicarea gradului de conștientizare a securității şi dezvoltarea unei culturi sociale în spațiul informațional este mai mult decât oricând necesar. În acest sens, am avut-o prezentă la eveniment pe **Ivana ARAPU**, care are peste 11 ani de experiență în domeniul de comunicații electronice şi tehnologia informației şi ne-a vorbit despre necesitatea dezvoltării unei Culturi de Securitate, și a nu percepe Securitatea doar ca o prescripție IT.

Ivana ARAPU, Şef Securitate Corporativă, Orange Moldova: *„Astăzi peste 90% dintre incidentele de securitate cibernetică la nivel internațional sunt atribuite erorilor umane. Motivul din spatele acestei observații nu este că sistemele de securitate cibernetică au performanțe slabe, ci mai degrabă o schimbare de paradigmă: criminalitatea cibernetică vizează acum ca vector primar oamenii mai degrabă decât sistemele informaționale. În timp ce oamenii pot fi ținta principală a atacurilor cibernetice, aceștia sunt și principalul lor adversar pentru a rezista amenințărilor în continuă creștere. Astfel trebuie să învățăm să prevenim, să identificăm și să raportăm fiecare incident pentru a fi protejați. Responsabili de securitatea personală, a celor apropiați și a mediului în care activăm este fiecare din noi."*

Modulul III. Conștientizarea securității cibernetice și ingineria socială

Institutul European de Studii Politice din Moldova (IESPM), în parteneriat cu Academia e-Governance au organizat în data de 21-22 ianuarie 2023, training-ul „Conștientizarea securității cibernetice".

În cadrul modulului "Conștientizarea securității cibernetice" Alexandru Angheluș (Prodefence CEO), specialist în domeniul securității cibernetice, auditor al sistemelor de management al securității informațiilor a abordat și a discutat împreună cu participanții de la training următoarele subiecte:

- Cum se întâmplă atacurile cibernetice?
- Cine le gândește și lansează?
- De ce se întâmplă incidente de securitate?
- Cum să răspundeți eficient la ele?
- Ce trebuie făcut pentru a vă proteja împotriva lor?

La training au participat doamne și domnișoare din instituțiile de stat, societatea civilă, instituții bancare, profesoare, studente înregistrate pe website-ul "Women in cyber".

Training-ul a relevat încă o dată stringența problemei de însușire a metodelor de protejare în spațiul cibernetic, de promovare și asimilare a principiilor igienei cibernetice, dar și necesitatea absolută de școlarizare a unor segmente importante din societatea noastră cu privire la securitatea cibernetică și reziliență în condițiile unor provocări serioase la adresa siguranței naționale. Participantele au avut posibilitatea să afle mai multe despre importanța educației cibernetice, conștientizarea pericolelor din mediul online, modalitățile de identificare a atacurilor cibernetice, acțiuni imediate și măsuri preventive, dispozitive personale/profesionale, conceptul "Zero trust" la nivel de utilizator etc.

Modulul IV. Asigurarea drepturilor omului pe platformele de socializare.

Regulamentul general privind protecția datelor (GDPR)

Institutul European de Studii Politice din Moldova (IESPM) a organizat în data de 28 ianuarie 2023, în format hybrid training-ul "Protecția datelor cu caracter personal" și "Asigurarea drepturilor omului în spațiul online" cu suportul Proiectului UE de Asistență rapidă pentru securitatea cibernetică în Republica Moldova, implementat de Academia de e-Guvernare din Estonia.

Datele personale sunt procesate în fiecare secundă la nivel mondial – la serviciu, în cadrul relaţiei cu autorităţile publice, în domeniul sănătăţii, în momentul tranzacţionării de bunuri sau servicii, în timpul efectuării călătoriilor în afara teritoriului naţional sau când posesorii datelor navighează pe internet.

Sergiu BOZIANU, expert național în domeniul protecției datelor cu caracter personal a făcut referință la cadrul legal cu privire la protecția datelor cu caracter personal în Republica Moldova și cum acestea sunt deseori încălcate, despre modalitățile de limitare a vieții private și publice, prin exemplificarea cazurilor concrete în care persoanele aflate în funcții publice au încălcat legile cu privire la protecția datelor cu caracter personal. Un accent deosebit a fost pus pe vulnerabilitatea noastră în mediul online și riscurile la care suntem supuși zilnic.

Ion IORDACHE, PECB ofițer de protecția datelor cu caracter personal (România), a enumerat diverse cazuri de încălcare a legilor cu privire la protecția datelor cu caracter personal, realizând un studiu comparativ dintre Republica Moldova și România. Un subiect aparte l-a constituit protecția datelor cu caracter personal al copiilor, o problemă nu doar pentru instituțiile de învățământ, dar și pentru părinți.

Sanda SANDU, fondatoarea Platformei pentru Inițiative de Securitate și Apărare (PISA), a analizat respectarea drepturilor omului în spațiul digital prin prisma noilor realități din mediul online și riscurile rezultate mai ales în contextul războiului din Ucraina și necesitatea prevenirii amenințărilor prin consolidarea securității digitale și cooperarea dintre instituții.

Training-ul a relevat încă o dată importanța igienii cibernetice, ca o responsabilitate individuală a fiecăruia, fiind și una dintre modalitățile de consolidare a culturii de securitate mai ales în rândul copiilor, care sunt foarte vulnerabili la amenințările din spațiul online.

Modulul V. Leadership în domeniul securității cibernetice

Institutul European de Studii Politice din Moldova (IESPM) a organizat în data de 2 februarie 2023, în format hybrid training-ul "Empowering women as leaders".

Leadership-ul și consolidarea drepturilor femeilor se pot realiza prin învățare, investiții și dezvoltare personală pe tot parcursul vieții. Care este primul pas? Cum pot fi perfecționate abilitățile de leader? Cum să faceți față provocărilor la locul de muncă și să vă dezvoltați strategii practice pentru dezvoltarea leadership-ului ? La aceste și alte întrebări au găsit răspuns participantele training-ului "Empowering women as leaders", care s-a desfășurat sub sloganul – **Descoperă leaderul din tine!**

Diana MOLODILO,expertă în leadership militar feminin și membră a Platformei pentru Inițiative de Securitate și Apărare în baza propriei experiențe profesionale, cercetărilor efectuate în domeniu și prin exemplificarea istoriilor de succes a leaderismului feminin, analizarea calităților necesare unui leader pentru a conduce eficient o echipă. O atenție deosebită s-a acordat dificultăților pe care

le întâmpină un leader feminin și modalitățile de a le depăși prin autocunoaștere și valori personale.

Andre SLOB, Șeful Securității Informaționale, Ofițer, Ministerul Apărării al Olandei prin prisma experienței sale militare a evidențiat trăsăturile definitorii a diferitor tipuri de leaderi, inegalitățile de gen în toate domeniile de activitate la care continuă să fie supuse femeile, dar și necesitatea de femei leader datorită calităților lor deosebite.

Viorica ȚÎCU, Decanul Facultății Relații Internaționale, Științe Politice și Jurnalism, ULIM, a realizat o analiză a gradului de reprezentare a femeilor în domeniul securității și apărării în Republica Moldova, punctând două dintre cele mai necesare abilități a unei femei leader: abilități de comunicare eficientă și reziliența ca o calitate esențială, care asigură succesul.

Alexandru BORDEA, Co-Fondator Angry Business a analizat strategiile, acțiunile și modalități de a te transforma într-un leader și de a menține această poziție prin asumare de riscuri și responsabilitate. Un subiect aparte l-a constituit independența financiară a femeilor și modalitățile de asigurare a acesteia.

La training au participat doamne și domnișoare din instituțiile de stat, societatea civilă, instituții bancare, profesoare, studenții/studentele Facultății Relații Internaționale, Științe Politice și Jurnalism (ULIM) înregistrate pe website-ul www.womenincyber.md..

Modulul VI. Sistemul de management al securității informațiilor (27001) și Managementul Riscurilor

În cadrul sesiunilor de training din 4 februarie 2023 au fost abordate următoarele subiecte: "Sistemul de management al securității informațiilor 27001", "Managementul Riscurilor" și exemplul Olandez de implementare.

Mihai-Ion DANȚIȘ, auditor certificat în Securitatea Informațiilor, Trainer (România) a definit și explicat conceptele de bază ale managementului securității informațiilor, standardele de securitate a informațiilor și dezvoltarea ISO 27001, cerințe ale standardului ISO 27001 pentru sistemul de management al securității informațiilor și relațiile cu alte standarde.

De asemenea, participantele la eveniment s-au familiarizat cu conceptul, principiilor și tendințelor ce guvernează managementul riscurilor și infrastructura internațională asociată în mediul economic și social actual, contextul în care operează managementul integrat al riscurilor organizației, a cerințelor legale și de reglementare, a standardelor de buna practică aplicabile organizațiilor, precum

și cu modalitățile de implementare și gestionare a unui sistem de management al riscurilor în organizație.

Rik VEENENDAAL, expert internațional în Securitate Cibernetică, a prezentat exemplul Olandei de implimentare și realizare a securității cibernetice și informaționale punctând cele mai importante etape, activități și cadrul legal creat și implementat în Olanda începând cu anul 2010, când a fost elaborată Strategia Națională a Securității Cibernetice, evidențiind bunele practici olandeze care ar putea fi preluate de către Republica Moldova.

Modulul VII. Introducere în dreptul internațional privind operațiunile cibernetice

TRAINING ONLINE

Institutul European de Studii Politice din Moldova (IESPM) a organizat la data de 8 februarie 2023, în format hybrid training-ul "Introduction to International Law on Cyber Operations" care a avut drept scop familiarizarea participantelor cu aspectele fundamentale în domeniul dreptului internațional privind operațiunile cibernetice.

Maiorul Nick Wobma a studiat Dreptul Informației (Information Law) la Universitatea din Amsterdam și la Universitatea Keio din Tokyo până în 2009.

Ulterior, în 2010 s-a alăturat forțelor armate olandeze. În 2015, a devenit consilier juridic - specializat în domeniul securității cibernetice în cadrul Agenției de Informații și Comunicații NATO inclusiv consilier pentru „NATO Cyber Incident Response Capacity".

Modulul VIII. Comunicarea strategică în contextul amenințărilor hibride/războiul hybrid

Institutul European de Studii Politice din Moldova (IESPM) în colaborare cu Orange Moldova au organizat la 11 februarie 2023, un atelier de instruire care a avut drept scop familiarizarea participanților și sporirea capacităților acestora în domeniul securității cibernetice, comunicării strategice, leadership precum și managementul crizelor.

Prima parte a atelierului de instruire a fost consacrată managementului crizelor. **Larisa GĂBUDEANU**, Expertă în domeniul securității cibernetice și protecția datelor personale și **Mircea-Constantin ȘCHEAU**, Doctor în Ordine Publică și Siguranță Națională le-au explicat participanților etapele gestionarii incidentelor de securitate în cadrul organizațiilor și aspectele practice de implementare a procesului intern privind gestionarea incidentelor.

Mihai GOIAN, drd. Școala Națională de Studii Politice și Administrative - SNSPA (București), consultant în cadrul "Institutului Național Democratic pentru Relații Internaționale din Washington" i-a familiarizat pe cei prezenți la eveniment cu aspectele teoretice ale securității cibernetice în contextul războiului hibrid cât și rolul acesteia în contracararea atacurilor hibride, exemplificând cazul Republicii Moldova.

Cristina SCHIMBOV, Președinta Asociației Femeilor din Poliție care a pus accentul pe leadership-ul feminin în contextul geopolitic actual și importanța comunicării în sectorul de securitate și apărare.

Tematica comunicării a fost continuată de către **Elena MÂRZAC**, Expertă în securitate și comunicare strategică, Co-fondatoare Platforma pentru Inițiative de Securitate și Apărare, în cadrul prezentării s-a referit la strategia de comunicare în domeniul securității cibernetice, gestionarea amenințărilor cibernetice, testarea și planificarea scenariilor și elaborarea planului de comunicare în cazul unei crize cibernetice.

Modulul IX. Introducere în diplomația cibernetică

TRAINING ONLINE

Institutul European de Studii Politice din Moldova (IESPM) a organizat la data de 17 februarie 2023, în format hybrid training-ul "Introduction to cyber diplomacy in tech context of various multilateral cooperations like EU, NATO, UN, OSCE and regional groupings" care a avut drept scop familiarizarea participantelor privind diplomația cibernetică în contextul diferitelor cooperări multilaterale precum UE, NATO, ONU, OSCE și grupări regionale.

Tadeusz CHOMICKI este diplomat de carieră și în prezent ambasador pentru afaceri cibernetice și tehnologie (Cyber & Tech Affairs) în cadrul Ministerului Afacerilor Externe al Poloniei. De asemenea, a fost ambasador în Republica Coreea (2001-2005) și ambasador în China și Mongolia (2009-2015). Domnul Chomicki a studiat la Universitatea din Varșovia, Universitatea Oxford și Institutul Universitar European și a primit un doctorat onorific în Hong Kong.

Modulul X. Certificare în securitate cibernetică (ISC2)

TRAINING ONLINE

Institutul European de Studii Politice din Moldova (IESPM) a organizat în perioada 18-19 februarie 2023, un training în format hybrid care a avut drept scop familiarizarea participantelor cu aspectele fundamentale privind securitatea rețelelor, controlul accesului fizic/logic, criptografia, securitatea rețelei, programele malware, principiile de securitate, planificarea continuității afacerii (BCP), planificarea recuperării în caz de dezastru (DRP) și conceptele de răspuns la incident.

Andy HUMPHRYS are o experiență de peste 20 de ani în domeniile tehnologiei informației și securității informațiilor/cibernetice. Deține un Master în Securitate Informațională acordat de Royal Holloway, Universitatea din Londra, împreună cu mai multe certificări din industrie (CISSP, CISM, CRISC, CISM, CEH, ISO/IEC 27001 Lead Implementer, ISO/IEC 27005 Senior Lead Risk Manager, Social Engineering Pentesting Professional).

Modulul XI. Tendințe emergente în criminalitatea cibernetică: investigarea criminalității cibernetice și criminalistica mobilă

Institutul European de Studii Politice din Moldova (IESPM) a organizat, la 25 februarie 2023 , în parteneriat cu Orange Moldova atelierul de lucru "Emerging Cybercrime Trends: Cybercrime Investigation and Mobile Forensics".

Criminalitatea cibernetică ia amploare pe zi ce trece. Cu cât numărul utilizatorilor de internet devine mai mare, cu atât crește și numărul de astfel de infracțiuni înregistrate. La sfârșitul anilor 1980, mai puțin de 1% din informațiile stocate din punct de vedere tehnologic din lume erau în format digital, în timp ce 94% în 2007, cu mai mult de 99% până în 2014.

Anul 2005 este considerat „începutul erei digitale", deoarece începând cu acest an, omenirea stochează mai multe informații în format digital, decât în format analog. Contextul și evoluția amenințărilor în acest domeniu, i-a determinat pe experți să-și unifice eforturile și să facă schimb de informații pentru a face față acestor pericole din mediul online.

Experții prezenți la eveniment **Mihai-Ion DANȚIȘ**, trainer, expert cybersecurity (România), **Ion GĂINA**, Șef al Secției Examinări Informaționale a Direcției Centru 1 a Centrului Tehnico-Criminalistic și Expertize Judiciare a IGP MAI (Republica Moldova) și **Gul ALTUNG**, expertă în securitate cibernetică, Ministerul Apărării (Olanda) au abordat și analizat într-o manieră multidimensională și din perspectiva țării unde activează, subiecte precum:

- Domeniul criminalității cibernetice: amenințări și tendințe;
- Amenințările actuale în domeniul fraudei online;
- Tendințele și posibilitățile criminalisticii digitate din Republica Moldova;
- Amenințări actuale și viitoare ale inteligenței artificiale (AI) și modalități de combatere a acestora în spațiul cibernetic;
- Criminalistica în domeniul dispozitivelor inteligente mobile;
- Probele obținute din dispozitivele mobile.

La final, a fost organizat exercițiul "Capture the Flag și Mobile Forensics" în care participanții au aplicat în practică cunoștințele privind amenințările cibernetice și s-au familiarizat cu modalitățile de intervenție în caz de criză.

Ceremonia de absolvire a programului de mentorat "WOMEN IN CYBER"

Programul de mentorat "WOMEN IN CYBER", care a reunit peste 200 de femei, s-a derulat pe parcursul a cinci luni și a reușit să sensibilizeze și să promoveze egalitatea de gen în sectorul securității cibernetice, oferind instruire, inspirație și motivare, prin împărtășirea cunoștințelor și prezentarea oportunităților unei cariere cibernetice de succes.

Invitații de onoare prezenți la eveniment: **Veronica ROȘCA**, Deputată, Comisia Juridică numiri și imunități, Parlamentul Republicii Moldova, **Olesea GARBUZ**, Ofițer de proiect, Institutul pentru Raportare de Război și Pace, **Floris VAN EIJK**,Chargé d'Affaires (Oficiul Ambasadei Regatului Olandei în Republica Moldova), **Epp MAATEN**, Team Leader, Proiectul de Asistență Rapidă pentru Securitate Cibernetică, implementat de Academia de e-Guvernare din Estonia, **Ivana ARAPU**, Șef Securitate Corporativă, Orange Moldova și **Viorica ȚÎCU**, Decana Facultății Relații Internaționale, Științe Politice și Jurnalism (ULIM)

au apreciat cu cele mai înalte calificative programul de mentorat, totodată menționând importanța securității cibernetice în actualul context geopolitic și evidențiind necesitatea creșterii numărului femeilor în domeniul asigurării securității cibernetice.

În cadrul evenimentului, participantele au prezentat propria viziune privind securitatea cibernetică adaptată la genul de activitate pe care îl profesează, completată de cunoștințele teoretice și abilitățile practice pe care le-au obținut pe parcursul Programului.

Daniela POPUȘOI, studenta Facultății Relații Internaționale, Științe Politice și Jurnalism (ULIM) le-a vorbit celor prezenți despre obstacolele și oportunitățile femeii lider; **Mihaela MELNIC**, studentă SNSPA și bibliotecară la Biblioteca Municipală "B.P. Hasdeu" i-a atenționat pe cei prezenți despre importanța securității cibernetice a Republicii Moldova în contextul războiului hybrid; **Gabriela DELEU**, specialist Calitate, Ingineria și Managementul Calității, a analizat alertele cu bombă din Chișinău evidențiind riscurile și soluțiile care există în practica internațională, **Mihaela BÎRLIBA**, jurist principal, Direcția Suport Juridic General, Departamentul Juridic, Moldova Agroindbank a atenționat celor prezenți despre identitatea online și consecințele acesteia asupra drepturilor omului; **Andreea GORAȘ**, studentă, Universitatea de Stat de Medicină și Farmacie "Nicolae Testemițanu" a menționat despre necesitatea integrării conceptului de securitate cibernetică în cadrul priorităților sistemului medical; **Alina MUȘET**, ofițer superior, Secția juridică a Agenției Asigurare Resurse și Administare Patrimoniu al Ministerului Apărării, Membra consiliului de administrare a Asociației Femeilor din Armata Națională a concluzionat - apărarea cibernetică reprezintă o prioritate tot mai mare pentru o dezvoltare durabilă.

Mentori

Natalia SPÎNU

Director, Institutul European de Studii Politice din Moldova (IESPM), fost șef al Centrului de Securitate Cibernetică al Guvernului (CERT-GOV) din cadrul Instituției Publice „Serviciul Tehnologia Informației și Securitate Cibernetică" cu o experiență de peste 10 ani în domeniul securității cibernetice și în multe arii ale acestuia, precum: managementul proiectelor TIC; dezvoltarea strategiei TIC; implementarea și auditul securității informațiilor; dezvoltarea politicii de securitate TIC.

Gül ALTUN

Expertă în securitate cibernetică, Gül Altun, are mai mult de 10 ani experiență în diverse domenii, cum ar fi, teste de penetrare, analiza rețelei criminalistice, analiza programelor virusate și diferite tipuri de conformități. Gül Altun este licențiată în Informare și Comunicare la Instituțiile de Învățământ din Leiden, Olanda.

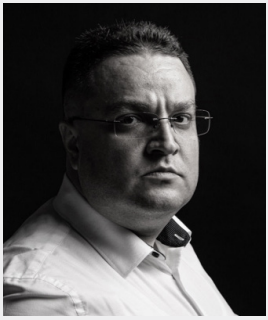
Elena MÂRZAC

Expertă în comunicare strategică și subiecte de securitate. Are o experiență de peste 15 ani în gestionarea proiectelor, comunicare și promovare în sectorul asociativ, public-privat și cel academic. Elena Mârzac este licențiată în Relații Internaționale, Master în Administrarea Afacerilor, Doctorandă în Relații Internaționale având subiectul de cercetare "Comunicarea Strategică în sectorul securității și apărării". A urmat cursuri la Școala NATO din Oberammergau (Germania) și Colegiul NATO din Roma (Italia).

Mihai GOIAN

Doctorand SNSPA(București) cu subiectul de cercetare "Implicații geopolitice ale războiului hibrid"; consultant în cadrul National Democratic Institute for International Affairs from Washington; fost consilier parlamentar(al Președintelui comisiei Românilor de Pretutindeni din Parlamentul României); peste 15 ani de experiență în web development.

Ion-Mihai DANȚIȘ



Trainer ISO 20000, ISO 22301, ISO 27001, ISO 27005, ISO 27032, ISO 27035, ISO 27701, ISO 31000 și DPO, cu o experiență de peste 20 de ani în tehnologia informației, iar ultimii 10 ani s-au concentrat pe securitatea informațiilor. Mihai a inițiat, dezvoltat și condus programe de securitate a informațiilor în calitate de ofițer de securitate a informațiilor pentru mai multe companii, responsabil cu protecția datelor și manager de proiecte IT.

Oana BUZIANU

Un profesionist pasionat în domeniul securității informațiilor, care a făcut din securitatea cibernetică o prioritate în cariera sa. Cu peste 20 de ani de experiență ca specialist în securitate cibernetică și o înțelegere profundă a proceselor de intelligence, Oana se concentrează pe trecerea de la reguli și politici la valori și etică, la a face ceea ce trebuie, chiar dacă nimeni nu se uită.

Sanda SANDU

Fondatoarea Platformei pentru Inițiative în Securitate și Apărare, Manager de program și expertă în securitate în cadrul Fundației Konrad Adenauer și Fellow în domeniul Drepturilor Omului în cadrul Wikimedia. Sanda Sandu are o experiență de peste 8 ani în domeniul societății civile și organizațiilor intenaționale, identificarea riscurilor de corupție, elaborarea politicilor de integritate, anticorupție și guvernarea sectorului de securitate.

Alexandru ANGHELUȘ

Alexandru Angheluș (Prodefence CEO) este specialist în domeniul securității cibernetice, auditor al sistemelor de management al securității informațiilor și al implementării Directivei NIS, specilizat în analizarea de fraude financiare cibernetice, aplicații malware, vulnerabilități ale infrastructurilor și atacuri cibernetice. Un aliat permanent al utilizatorilor de tehnologie, prin intermediul analizelor/avertizărilor de securitate cibernetică, precum și prin intermediul cursurilor de securitate cibernetică oferite.

Ion IORDACHE

Economist de profesie și absolvent al unei școli militare de ofițeri cu specializarea în logistică, am peste 20 de ani de experiență profesională în activități de consultanță și educație profesională a adulților în domenii ca: securitatea privată, protecția datelor cu caracter personal (GDPR) fiind certificat ca "PECB Data Protection Officer" și în mai multe sisteme de management (ISO 9001, ISO/IEC 27001, ISO 28000 și ISO 37001) pentru care dețin certificări "PECB Certified Lead Implementer" și "PECB Certified Lead Auditor".

Sergiu BOZIANU

Expert național în domeniul protecției datelor cu caracter personal

Director ,,Data Protection Law Firm" (www.gdpr.md)

Președinte Asociația pentru Protecția Vieții Private (www.privacy.md)

Rik VEENENDAAL

Rik s-a alăturat forțelor armate în 1978 și a servit în Corpul Marin Regal al Țărilor de Jos în diferite părți ale lumii, inclusiv în misiuni în Cambodgia și Irak. Din 2006 activează în domeniul securității IT și din 2012 până în 2020, a activat în calitate de coordonator senior în Echipa Computer Emergency Response (CERT) Ministerului Apărării din Regatul Țărilor de Jos.

a

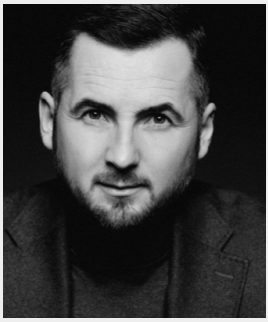
Nick WOBMA

Maior Nick Wobma a studiat Dreptul Informației (Information Law) la Universitatea din Amsterdam și la Universitatea Keio din Tokyo până în 2009. Ulterior, în 2010 s-a alăturat forțelor armate olandeze. În 2015, a devenit consilier juridic - specializat în domeniul securității cibernetice în cadrul Agenției de Informații și Comunicații NATO inclusiv consilier pentru „NATO Cyber Incident Response Capacity".

Viorica ȚÎCU

Decan al Facultatii Relaţii Internaţionale, Ştiinţe Politice și Jurnalism, Universitatea Liberă Internaţională din Moldova (ULIM), absolventă a Școlii Naţionale de Studii Politice şi Administrative, Departamentul Relaţii Internaţionale şi Integrare Europeană, Bucureşti, România; Absolventă a Facultăţii de Istorie, Universitatea de Stat din Moldova; Studii Masterat în istorie (Studii Sud-Est Europene), Catedra UNESCO, Universitatea de Stat din Moldova.

Alexandru BORDEA



Business trainer, consultant cu 17 ani experiență; Peste 5.000 de antreprenori consultați si peste 300 companii împachetate; Peste 180 de antreprenori în programul de mentorat; Fondator BRIDGE, Evenda si cofondator AngryBusiness.

Mircea-Constantin ȘCHEAU

Doctor în Ordine Publică și Siguranță Națională, cu o temă de interes pentru domeniul economic și de securitate - ”Criminalitatea informatică privind transferurile financiare”, care a primit „Premiul Victor Slăvescu” acordat de Academia Română. Autor / coautor a trei volume, peste cincizeci de articole științifice referitoare la management, aplicarea legii, infrastructuri critice, tehnologia informației, inteligență artificială, apărare, securitate cibernetică, lector în numeroase conferințe internaționale.

Larisa GĂBUDEANU

Este un profesionist în domeniul securității cibernetice și protecția datelor personale, în prezent în cadrul unei bănci parte dintr-un grup regional din Europa. Este autor/coautor al mai multor cărți, inclusiv despre Tehnologia informației și managementul riscului de confidențialitate, autor de articole stiintifice, lector invitat și vorbitor la conferințe naționale și internaționale. De asemenea, are o vastă experiență ca avocat într-o firmă internațională de avocatură, consilierea clienților internaționali și coordonarea proiectelor legate de dreptul bancar, dreptul IT, criminalitatea cibernetică și probleme de protecție a datelor.

Andy HUMPHRYS

Andy are o experiență de peste 20 de ani în domeniile tehnologiei informației și securității informațiilor/ cibernetice. Deține un Master în Securitate Informațională acordat de Royal Holloway, Universitatea din Londra, împreună cu mai multe certificări din industrie (CISSP, CISM, CRISC, CISM, CEH, ISO/IEC 27001 Lead Implementer, ISO/IEC 27005 Senior Lead Risk Manager, Social Engineering Pentesting Professional).

Tadeusz CHOMICKI

Tadeusz Chomicki este diplomat de carieră și în prezent ambasador pentru afaceri cibernetice și tehnologie (Cyber & Tech Affairs) în cadrul Ministerului Afacerilor Externe al Poloniei. De asemenea, a fost ambasador în Republica Coreea (2001-2005) și ambasador în China și Mongolia (2009-2015). Domnul Chomicki a studiat la Universitatea din Varșovia, Universitatea Oxford și Institutul Universitar European și a primit un doctorat onorific în Hong Kong.

Directiva NIS 2 și impactul său asupra organizațiilor

Ion-Mihai Dancțiș

Director executiv Octalogik

Directiva NIS 2 este o actualizare a Directivei NIS (Network and Information Systems) originală, care a fost primul set de reguli de securitate cibernetică la nivelul UE. Această directivă a fost adoptată pentru a face față provocărilor în creștere în domeniul securității cibernetice și pentru a îmbunătăți reziliența rețelelor și sistemelor de informații esențiale în Uniunea Europeană.

Impactul Directivelor NIS 2 asupra organizațiilor este semnificativ din mai multe motive:

Extinderea Scopului: Directiva NIS 2 extinde domeniul de aplicare al directivei originale, incluzând mai multe sectoare și servicii esențiale, cum ar fi entitățile din domeniul alimentar, al apei și sectorul medical. Acest lucru înseamnă că mai multe organizații vor fi acum supuse cerințelor de securitate cibernetică.

Cerințe Mai Stricte: Directiva NIS 2 introduce cerințe mai stricte pentru organizații în ceea ce privește măsurile de securitate pe care trebuie să le implementeze. Acestea includ cerințe pentru gestionarea riscurilor, politici de securitate, proceduri de incident management și audituri.

Raportarea Incidentelor: Organizațiile sunt obligate să raporteze incidentele de securitate cibernetică într-un termen mai scurt decât cel prevăzut în directiva originală. Acest lucru va necesita ca organizațiile să aibă sisteme mai bune de detectare și răspuns la incidente.

Sancțiuni: Directiva NIS 2 introduce sancțiuni mai severe pentru nerespectarea cerințelor. Acest lucru ar putea avea un impact financiar semnificativ asupra organizațiilor care nu îndeplinesc cerințele.

Cooperare: Directiva NIS 2 încurajează cooperarea între statele membre ale UE și schimbul de informații despre amenințări și incidente de securitate cibernetică. Acest lucru va ajuta organizațiile să fie mai bine pregătite și să răspundă mai eficient la amenințările cibernetice. Directiva privind securitatea rețelelor și sistemelor informatice a UE (NIS 2) a fost adoptată de Parlamentul European la 6 iulie 2021 și își propune să îmbunătățească securitatea cibernetică generală

a UE prin stabilirea de noi cerințe și obligații pentru anumite organizații. În decembrie 2022, Consiliul European a adoptat o recomandare privind o abordare de coordonare la nivelul UE pentru consolidarea rezilienței a infrastructurilor critice, în care statele membre sunt invitate să accelereze lucrările de pregătire pentru transpunerea și aplicarea NIS 2 și a Directivei privind reziliența entităților critice (CER).

Ca și elemente principale regăsim următoarele:

1. Domeniu de aplicare: Directiva NIS 2 se aplică operatorilor de servicii esențiale (OES) și furnizorilor de servicii digitale (DSP) care operează în UE. OES sunt definite ca entități care furnizează servicii critice, cum ar fi energie, transport, servicii bancare și asistență medicală, în timp ce DSP-urile sunt definite ca entități care furnizează servicii digitale, cum ar fi piețele online, serviciile de cloud computing și motoarele de căutare.

2. Cerințe: Directiva cere OES și DSP să ia măsuri pentru a gestiona riscurile de securitate cibernetică, inclusiv implementarea măsurilor de securitate adecvate, notificarea autorităților cu privire la orice incident semnificativ de securitate și stabilirea planurilor de răspuns la incidente. Directiva cere, de asemenea, OES și DSP să numească un punct de contact desemnat pentru a asigura legătura cu autoritățile naționale.

3. Aplicarea: Directiva stabilește un cadru pentru statele membre UE pentru a pune în aplicare cerințele directivei, inclusiv sancțiuni pentru nerespectare.

Directiva NIS 2 este concepută pentru a aborda o serie de riscuri și provocări de securitate cibernetică cu care se confruntă UE, iar acestea includ următoarele:

1. Atacurile cibernetice asupra infrastructurii critice: Directiva își propune să îmbunătățească reziliența infrastructurii critice, cum ar fi sistemele energetice, de transport, bancare și de sănătate, la atacurile cibernetice care ar putea perturba serviciile esențiale și ar putea cauza prejudicii semnificative.

2. Amenințări transfrontaliere la adresa securității cibernetice: Directiva urmărește să abordeze provocările amenințărilor transfrontaliere la adresa securității cibernetice, care pot afecta mai multe state membre ale UE și necesită răspunsuri coordonate.

3. Riscurile privind securitatea cibernetică a furnizorilor de servicii digitale: directiva stabilește noi cerințe pentru furnizorii de servicii digitale, cum ar fi piețele online, serviciile de cloud computing și motoarele de căutare, pentru a gestiona riscurile de securitate cibernetică care ar putea compromite securitatea datelor utilizatorilor.

4. Măsuri insuficiente de securitate cibernetică: directiva urmărește să abordeze riscurile prezentate de măsurile insuficiente de securitate cibernetică luate de OES și DSP, care le-ar putea face vulnerabili la atacuri cibernetice și la scurgeri de date.

5. Lipsa planificării răspunsului la incident: directiva cere OES și DSP să aibă planuri de răspuns în cazul incidentelor semnificative de securitate cibernetică. Acesta are scopul de a îmbunătăți capacitatea organizațiilor de a răspunde rapid și eficient la atacurile cibernetice și de a minimiza impactul asupra serviciilor și datelor critice.

6. Comunicare inadecvată între organizații și autorități: directiva cere OES și DSP să numească un punct de contact desemnat pentru a asigura legătura cu autoritățile naționale în cazul unui incident semnificativ de securitate cibernetică. Acesta are scopul de a îmbunătăți comunicarea și colaborarea dintre organizații și autorități și de a facilita un răspuns coordonat la amenințările de securitate cibernetică.

Impactul Directivei NIS 2 asupra întreprinderilor va depinde de industria și dimensiunea acestora. OES și DSP-urile vor trebui să își evalueze măsurile actuale de securitate cibernetică și să determine dacă trebuie să facă îmbunătățiri pentru a se conforma cerințelor directivei. Ei vor trebui, de asemenea, să stabilească planuri de răspuns la incident și să numească un punct de contact desemnat. Mai jos, enumerăm câteva dintre provocările cheie necesare întreprinderilor pentru a se conforma cu Directiva NIS 2. Respectarea Directivei NIS 2 poate fi o provocare pentru întreprinderi, în special pentru cele care implimentează directiva pentru prima dată.

Unele dintre provocările cheie în materie de conformitate includ:

1. Înțelegerea domeniului de aplicare: una dintre provocările principale pentru întreprinderi este de a determina dacă acestea intră în domeniul de aplicare al directivei ca OES sau DSP. Acest lucru necesită o evaluare atentă a naturii afacerii și a serviciilor pe care le oferă.

2. Evaluarea riscului de securitate cibernetică: directiva solicită OES și DSP să-și evalueze riscurile de securitate cibernetică și să pună în aplicare măsuri de securitate adecvate. Acest lucru poate fi o provocare pentru companiile care nu au echipe dedicate de securitate cibernetică sau care nu au expertiza necesară pentru a efectua o evaluare amănunțită.

3. Planificarea răspunsului la incident: OES și DSP trebuie să aibă planuri de răspuns la incident în cazul unui incident de securitate semnificativ. Dezvoltarea și implementarea unui plan de răspuns eficient poate fi o provocare, în special pentru companiile care nu s-au concentrat anterior pe securitatea cibernetică.

4. Punct de contact desemnat: directiva cere OES și DSP să numească un punct de contact desemnat pentru a asigura legătura cu autoritățile naționale. Acest lucru poate fi o provocare pentru companiile care operează în mai multe țări și trebuie să își coordoneze răspunsul la incidentele de securitate cibernetică.

5. Alocarea resurselor: Conformitatea cu Directiva NIS 2 poate impune întreprinderilor să investească în noi tehnologii, personal și procese pentru a-și îmbunătăți măsurile de securitate cibernetică. Acesta poate fi un cost semnificativ pentru unele întreprinderi, în special pentru întreprinderile mici și mijlocii (IMM-uri).

6. Conformitatea transfrontalieră: OES și DSP care operează în mai multe state membre ale UE se pot confrunta cu provocări în respectarea diferitelor legi și reglementări naționale în materie de securitate cibernetică, precum și în coordonarea răspunsului la incident la nivel transfrontalier.

Astfel, respectarea Directivei NIS 2 va necesita investiții în tehnologie, personal și procese. Pentru companiile care implimentează pentru prima dată, aceasta ar putea fi un cost semnificativ. Cu toate acestea, nerespectarea directivei ar putea duce la amenzi și prejudicii, la adresa reputației companiei. Practicile cheie de afaceri care pot fi adoptate în conformitate cu directiva NIS 2 sunt derivate din provocările de conformitate enumerate:

1. Elaborarea unui plan de răspuns la incident: Elaborați și implementați un plan eficient de răspuns în cazul unui incident de securitate semnificativ. Acest plan ar trebui să includă proceduri clare pentru identificarea, limitarea și atenuarea impactului unui incident de securitate cibernetică.

2. Numiți un punct de contact desemnat: desemnați un punct de contact desemnat pentru a asigura legătura cu autoritățile naționale în cazul unui incident semnificativ de securitate cibernetică. Această persoană ar trebui să fie familiarizată cu planul de răspuns la incident și să aibă autoritatea de a lua decizii într-o criză.

3. Instruirea angajaților: Instruiți angajații cu privire la cele mai bune practici de securitate cibernetică și măsurile de securitate specifice și procedurile de răspuns la incidente implementate de companie. Acest lucru va ajuta să vă asigurați că toată lumea din organizație este conștientă de rolul și responsabilitățile lor în menținerea securității cibernetice.

4. Revizuirea și actualizarea în mod regulat a măsurilor de securitate cibernetică: revizuiți și actualizați în mod regulat măsurile de securitate cibernetică pentru a vă asigura că rămân eficiente și actualizate cu evoluția riscurilor și amenințărilor de securitate cibernetică.

5. Înțelegerea domeniului de aplicare: stabiliți dacă afacerea dvs. intră în domeniul de aplicare al directivei ca OES sau DSP. Acest lucru necesită o evaluare atentă a naturii afacerii și a serviciilor pe care le oferă.

6. Efectuarea unei evaluări detaliate a riscurilor de securitate cibernetică: Efectuarea unei evaluări amănunțite a riscurilor de securitate cibernetică pentru a identifica potențialele amenințări, vulnerabilități și riscuri pentru afacerea dvs. Acest lucru va ajuta afacerea cuiva să determine măsurile de securitate adecvate care trebuie implementate pentru a gestiona riscurile.

7. Implementarea unei măsuri de securitate adecvate: implementați măsuri de securitate adecvate pe baza rezultatului evaluării riscului de securitate cibernetică. Acestea pot include măsuri de securitate a rețelei, controale de acces, criptare și instrumente de monitorizare.

8. Căutați expertiză externă: Luați în considerare căutarea de expertiză externă, cum ar fi consultanți în domeniul securității cibernetice, pentru a ajuta la respectarea Directivei NIS 2. Acest lucru poate oferi expertiză și resurse suplimentare pentru a ajuta la gestionarea riscurilor de securitate cibernetică.

Concluzie:

Directiva NIS 2 încearcă să abordeze o serie de riscuri și provocări de securitate cibernetică care ar putea avea un impact semnificativ asupra infrastructurii critice, serviciilor digitale și informațiilor sensibile din UE. Prin stabilirea de noi cerințe și obligații pentru OES și DSP, directiva își propune să îmbunătățească măsurile de securitate cibernetică și să sporească reziliența UE la amenințările cibernetice.

Astfel, Directiva NIS 2 va asigura o Europă mai sigură și mai puternică prin extinderea semnificativă a sectoarelor și a tipurilor de entități critice care intră în domeniul său de aplicare. Acestea includ furnizorii de rețele și servicii publice de comunicații electronice, servicii de centre de date, managementul apelor uzate și a deșeurilor, producția de produse critice, servicii poștale și de curierat și entități ale administrației publice, precum și sectorul sănătății în general. În plus, va consolida cerințele de management al riscului de securitate cibernetică pe care companiile sunt obligate să le respecte, precum și va simplifica obligațiile de raportare a incidentelor cu prevederi mai precise privind raportarea, conținutul și durata de timp. În general, Directiva NIS 2 este un pas către îmbunătățirea securității cibernetice incluzive a UE.

Deși poate reprezenta provocări pentru unele companii, este în cele din urmă în interesul tuturor să existe măsuri de securitate cibernetică mai robuste pentru a proteja infrastructura critică și informațiile sensibile.

Apărarea cibernetică - reper de gestionare a securității cibernetice

„Câștigătorii nu renunță. Cei care renunță nu câștigă. Dacă nici nu câștigi și nici nu renunți, lucrezi în securitate cibernetică”

Oana BUZIANU

Specialist în Securitate Cibernetică, permanent preocupată de etică și de integritatea datelor personale; susțin cu tărie identificarea slăbiciunilor din orice sistem, înainte ca ele sa fie exploatate de către criminalii cibernetici.

Există sute de documentații, standarde, ghiduri, proceduri, recomandări privind măsurile tehnice care pot fi puse în aplicare pentru asigurarea securității cibernetice, respectiv a apărării cibernetice, astfel încât să permită gestionarea cuprinzătoare a riscurilor. Riscurile cibernetice depășesc capacitatea individuală de răspuns, obligând organizațiile să coopereze integrat spre atingerea unui scop comun: securitatea cibernetică.

Securitatea cibernetică este un proces complex, existent în toate ciclurile de viață ale tehnologiei, nu doar o serie de măsuri care pot fi aplicate din exterior, cu care să se suplinească lipsa intrinsecă de securitate a tehnologiei. Trebuie să fie gândită și proiectată în mod echilibrat, începând din stadiile de cercetare, design și producție, pentru asigurarea unei fundații stabile (denumită și security-by-design sau built-in security), continuând în stadiul de utilizare (cu măsuri de prevenție, protecție și management al proceselor) și încheind cu acțiuni finalizatoare, care preîntâmpină scurgerea de informații sau utilizarea necorespunzătoare post eveniment de securitate. Scopul de ansamblu vizează obținerea unei capacități predictive, care să alerteze cu privire la apariția unui incident de securitate cibernetică, să prevină manifestarea acestuia și să gestioneze corespunzător evoluția sa, pentru a limita pe cât posibil efectele nedorite pe care acesta le generează. Ca atare, este necesar ca măsurile de securitate cibernetică să respecte într-un mod armonizat cerințele de proactivitate, reactivitate și integrare a eforturilor de protecție.

În funcție de unghiul din care privim, termenii de securitate çi apărare cibernetică

se suprapun. În esență, securitatea are un caracter de proactivitate reprezentând măsurile luate permanent pentru buna funcționare a sistemelor în condiții de siguranță și protecție, apărarea având capacitatea de a preveni și răspunde situațiilor critice. Securitatea cibernetică înțelege apărarea ca pe un mecanism și de preîntâmpinare și de răspuns la atacuri cibernetice. De aceea, este nevoie să înțelegem câteva principii de bază pe care le avem de urmărit, ca scopuri de implementare și funcționare a mecanismelor de securitate cibernetică în infrastructurile pe care le protejăm.

Descoperirea timpurie a activităților malware se realizează, în principal, prin două metode: prin automatizare și prin explorare.

Automatizare și threat hunting[1]

Automatizarea presupune instalarea unor senzori care să capteze modul de funcționare al echipamentelor tehnologice, preluarea și analiza corelată a acestora în baza unor algoritmi și configurarea unor procese de alertare automată. Întregul flux de analiză și identificare automatiza necesită eforturi consistente pentru configurarea inițială, mentenanță și urmărire, însă asigură cea mai cuprinzătoare imagine asupra proceselor, din punct de vedere al securității cibernetice.

În completare, pentru acele incidente care escaladează mecanismele de detecție și procesare automată, este necesară dezvoltarea și operaționalizarea unor procese de explorare manuală, vânătoare a amenințărilor, sau threat hunting. Acestea sunt realizate de specialiști dedicați, care analizează permanent fluxurile de lucru (în paralel cu mecanismele de detecție automatizată) și investighează sistemele și rețelele tehnologice, respectiv spațiul de Intelligence, în căutarea indicatorilor care pot avertiza cu privire la posibilitatea reală de manifestare a unor incidente cibernetice. Este ideal să automatizăm mecanismele de monitorizare, detecție și răspuns rapid la incidentele de securitate cibernetică. Orice acțiune care poate fi automatizată, trebuie să ruleze pe baza unor algoritmi de urmărire liniari (și/sau comportamentali), astfel încât să se asigure descoperirea pattern-urilor malițioase cunoscute și pe cele de căutare proactivă și iterativă prin rețele pentru a detecta și izola amenințările avansate care se sustrag soluțiilor de securitate existente care modifică activitea internă a rețelei de la normal/ uzual.

Toate mecanismele automatizate au nevoie de o configurare corespunzătoare (care să asigure corectitudinea algoritmilor și filtrelor de detecție) și de administrare continuă. Mai mult, în condițiile în care unele atacuri cibernetice sunt generate sau facilitate de instrumente autonome care dispun de inteligență

artificială, devine necesar ca echipamentele de securitate să poată ține piept nivelului de complexitate al incidentelor/ atacurilor, prin capabilități similare și configurări corespunzătoare. Aceasta presupune completarea capabilităților tehnice automatizate cu capabilități de threat hunting, dependente de expertiza analiștilor tehnici, care completează activitățile de configurare și administrare a tehnologiilor de securitate cibernetică cu activități de explorare, investigare, testare și verificare, în scopul preîntâmpinării și prevenției incidentelor cibernetice.

Există numeroase soluții de securitate cibernetică la toate nivelurile care prelucrează, analizează și gestionează evenimentele de securitate și care oferă o protecție rezonabilă pentru majoritatea riscurilor tehnice, având însa dezavantajul de a nu răspunde întotdeauna necesităților de securitate specifice contextului unic al fiecărei infrastructuri IT. Aceste soluții de securitate cibernetică trebuie să fie implementate în mod inteligent, urmărind un echilibru de complexitate și funcționalitate corespunzător și asigurând reziliența în fața riscurilor specifice. Un exemplu ar fi defense-in-depth (sau apărarea în profunzime), care se bazează pe asigurarea securității stratificate, plasând obiectivul cel mai important în centrul nivelurilor de protecție.

Securitatea fizică – deși nu pare a avea legătură cu domeniul cibernetic – este primul nivel de protecție al infrastructurii IT, asigurând condițiile fizice necesare funcționării nealterate și neîntrerupte a acesteia. Să nu uităm că orice aplicație software este susținută de echipamente hardware, a căror protecție fizică este absolut necesară pentru asigurarea serviciilor dorite și care devine ineficientă în lipsa procedurilor și regulilor de acțiune și conduită individuale sau organizaționale. Pentru că nu protecția fizică este fundamentală, ci decizia omului privind gestionarea acesteia, regulile și procedurile fiind o formă de asumare a conștientizării și trasabilității acțiunilor. În lipsa acestora, eforturile de prevenire și reacție la incidentele cibernetice sunt zădărnicite, lăsând cale liberă manifestării incidentelor sau exploatărilor din interior.

Primul nivel tehnologic asupra căruia trebuie să ne îndreptăm atenția – din perspectiva nevoii de protecție – este cel al tehnologiei informaționale (IT&C). În mod special, trebuie să avem în vedere rețelele cu conexiune la Internet și pe cele administrative (care găzduiesc serviciile de bază organizaționale), întrucât reprezintă principalele căi de transmitere a malware-ului. Rețelele informatice trebuie să aibă implementate mecanisme de security-by-design)[3], respectiv să fie gândite, concepute, construite, configurate și exploatate cu respectarea tuturor cerințelor de securitate specifice, pentru a asigura protecția de-a lungul întregului ciclu de viață. Security-by-design devine din ce în ce mai mult abordarea convențională de dezvoltare pentru a asigura securitatea

și confidențialitatea sistemelor software. În această abordare, securitatea este luată în considerare și integrată în sistem la fiecare nivel și începe cu un design robust al arhitecturii. Deciziile de proiectare arhitecturală de securitate se bazează pe strategii, tactici și modele de securitate binecunoscute definite ca tehnici reutilizabile pentru atingerea unor preocupări specifice de calitate. Modelele de securitate oferă soluții pentru aplicarea cerințelor necesare de autentificare, autorizare, confidențialitate, integritate a datelor, confidențialitate, responsabilitate, disponibilitate, siguranță și non- repudiere, chiar și atunci când sistemul este atacat.

Rețelele trebuie să fie percepute ca o tehnologie în sine, care însumează echipamente și le valorifică într-un context de complexitate superioară. Aici, măsurile de securitate sunt aplicate atât la nivel de echipament (endpoint) și utilizator (enduser), cât și în mod integrat (la nivel de rețea).

Măsurile de protecție ale rețelelor OT (Operational Technology) sunt adaptate specificului echipamentelor și presupun un nivel de precauție ridicat, care poate obliga la funcționarea total independentă a acestora, în lipsa conexiunilor fizice cu orice alte rețele sau echipamente tehnologice. Acțiunile în scopul asigurării funcționării și protecției acestora sunt bine documentate și procedurate, pentru a asigura o cât mai mică expunere la erori sau la exploatare nedorită.

Mecanismele de securitate cibernetică aplicate la nivelul rețelelor OT pot fi integrate cu cele prevăzute pentru alte tipuri de rețele, în scopul monitorizării și detecției centralizate a incidentelor cibernetice, însă trebuie avută în vedere implementarea de mecanisme de comunicații într-un singur sens (care limitează fizic transmisia de date din rețeaua OT către rețelele cu nivel inferior de criticalitate).

Pentru a dobândi un grad ridicat de securitate cibernetică, este dezirabilă integrarea capacităților de monitorizare și detecție a incidentelor cibernetice la nivelul tuturor tipurilor de tehnologii (informatice, operaționale și emergente) care să permită dobândirea unei vizibilități extinse a echipamentelor și rețelelor deținute și a unei capacități ridicate de prevenție și contracarare a manifestării riscurilor cibernetice.

Tehnologiile emergente depind de transformarea digitală, de inteligența artificială, de transformarea capacităților de procesare informațională de la binar la cuantic, de automatizare și autonomizare, etc.). Aceste noi tehnologii sunt și vor fi prezente în toate peisajele tehnice care ne înconjoară, făcând ca separația dintre tehnologia informatică și cea operațională să fie din ce în ce mai greu de respectat și de gestionat. Actuala revoluție industrială se va resimți în toate tipurile de echipamente și rețele pe care le utilizăm, crescând

conectivitatea în mod exponențial și gestionând procesarea informațiilor în mod centralizat, în spiritul Big Data. Din păcate, multe dintre aceste tehnologii emergente nu au implementate mecanisme de securitate, din cauza necesităților funcționale și de performanță ridicată, ceea ce pe termen lung predispune la destabilizarea peisajului tehnologic în ansamblu.

Securitatea noilor tehnologii va trebui tratată în corelație cu tehnologiile informatice și operaționale, asigurând eficiența maximă atât la nivel de endpoint, cât și de ansamblu, eliminând pe cât posibil punctele slabe/ vulnerabile care pot pune în pericol echipamentele, rețelele și întregul ecosistem din care fac parte.

Modelul defense-in-depth (apărării în adâncime) este necesar, dar nu este suficient pentru abordarea completă a apărării cibernetice, întrucât relevă o gândire tradițională, de protejare a infrastructurilor tehnologice aflate în spațiul propriu (on- premises)[2].Tehnologiile de care dispun organizațiile în prezent depășesc granițele incintelor proprii, migrând spre cloud și spre servicii software care rulează în platforme hardware dinamice (de ex. tehnologia 5G care presupune dezvoltarea unei infrastructuri hardware de rețea care să permită gestionarea flexibilă a serviciilor software suportate), impunând adaptarea mentalităților de securitate cibernetică spre abordări care gestionează încrederea(drepturi de acces, niveluri de privilegii, filtrare de tip firewall, control la nivelul fiecărei acțiuni))[3]. Modelele și conceptele arhitecturale pentru asigurarea securității cibernetice evoluează (Zero-Trust)[5]. Software Defined Perimeter)[4]. etc.) în încercarea de a răspunde în mod adaptat și cât mai eficient provocărilor introduse de riscurile tehnologice. Zero-Trust (Încredere-Zero) este un model de securitate centrat pe date, care se concentrează mai puțin pe infrastructura IT fizică și mai mult pe activitatea din cadrul rețelei. Cel mai important lucru pentru infractorii cibernetici sunt activele digitale ale țintelor atacurilor, reprezentate în mare parte ca date. Prin urmare, organizațiile trebuie să protejeze în primul rând sursa datelor, transmiterea și stocarea acestora.

O strategie de încredere-zero impune permisiuni stricte de acces, controale și permisiuni. Utilizatorii au acces limitat la anumite active digitale. Utilizatorii pot vizualiza și accesa doar componentele de infrastructură necesare pentru a îndeplini o sarcină atribuită. Această abordare este o strategie de control al accesului determinată de riscuri.

Un perimetru definit de software (SDP) reprezintă o modalitate de a ascunde infrastructura conectată la Internet (servere, routere, etc.), astfel încât părțile externe și atacatorii să nu o poată vedea, indiferent dacă este găzduită on-premise sau în cloud. Scopul abordării SDP este de a baza perimetrul rețelei pe software și nu pe hardware. O companie care folosește un SDP își acoperă, în

esență, serverele și alte infrastructuri, astfel încât nimeni să nu le poată vedea din exterior; cu toate acestea, utilizatorii autorizați pot accesa în continuare infrastructura.

În concluzie, indiferent de modelele de securitate implementate, măsurile de securitate cibernetică sunt obligatorii. Acestea pot fi tehnice (în legătură cu tehnologia), fizice (în legătură cu spațiul fizic care găzduiește și protejează tehnologia) și administrative (relative la procesele organizaționale și deciziile umane), scopul final fiind ca setul de măsuri implementate să prevină incidentele cibernetice (materializări ale riscurilor cibernetice).

Însă, datorită dificultăților tehnice, financiare și decizionale de a implementa un nivel de performanță ridicat în raport cu necesitățile reale (măsurile de securitate sunt proporționale cu riscurile analizate) și datorită incapacității umane de a gestiona evenimentele înainte ca acestea să se producă, de cele mai multe ori predicția este greu de atins.

Pentru prevenirea materializării riscurilor sunt necesare o serie de măsuri de securitate cibernetică proactive, care includ printre altele:

- Dezvoltarea de reglementări, strategii, standarde, proceduri, politici și controale de securitate cibernetică.
- Managementul integrat al riscurilor de securitate cibernetică, planificarea răspunsului la incidente cibernetice și la situații de criză, dezvoltarea de proceduri în caz de urgență
- Monitorizarea conformității și desfășurarea de audituri procedurale
- Evaluarea și monitorizarea securității cibernetice a infrastructurilor tehnologice
- Formarea culturii de securitate cibernetică prin creșterea nivelului de conștientizare, educație și instruire, precum și prin exersarea capacității de răspuns la incidente cibernetice
- Proiectarea și dezvoltarea (incluzând configurarea, administrarea și mentenanța) capabilităților tehnice specializate pentru pregătirea, prevenția și reacția la incidentele de securitate cibernetică
- Desfășurarea de activități de cercetare-dezvoltare pentru identificarea soluțiilor de securitate cibernetică optime, precum și asimilarea tehnologiilor digitale emergente
- Cooperarea și schimbul de informații pentru pregătirea și prevenția incidentelor de securitate cibernetică

— Adaptarea managementului organizațional la necesitățile de gestionare a securității cibernetice.

Incidentele cibernetice se datorează gestionării necorespunzătoare (sau exploatării intenționate a tehnologiei), dar interacțiunii umană/ inginerie socială. Pentru a putea obține un nivel corespunzător de securitate cibernetică, este necesar să luăm măsurile care se impun pentru un management corespunzător al riscurilor cibernetice, asigurând deopotrivă evaluarea riscurilor, prevenirea și managementul incidentelor cibernetice. Riscurile pot fi neacceptate, acceptate, atenuate, sau transferate. În final, managementul riscului reprezintă o decizie cu privire la modalitățile de tratare a situațiilor de risc în funcție de specificitățile acestora, astfel încât să fie asigurat un nivel optim de securitate și siguranță.

Dacă au avut loc incidente cibernetice, se impun o serie de măsuri de securitate reactive, incluzând:

— Exploatarea, valorificarea și adaptarea capabilităților tehnice specializate

— Analiza și investigarea evenimentelor cibernetice

— Activități de threat hunting

— Managementul integrat al incidentelor de securitate cibernetică, incluzând detecția, răspunsul, reducerea, blocarea, recuperarea, remedierea, raportarea și ținerea evidenței incidentelor

— Colaborarea și coordonarea unitară pentru răspuns la incidentele cibernetice.

Dincolo de aspectele tehnice ale apărării cibernetice, există o serie de implicații umane de care trebuie să ținem cont în procesul implementării efective a planurilor, arhitecturilor și măsurilor specifice. Nu întotdeauna corectitudinea tehnică este cea care descrie realitatea din activitate, cât implicațiile practice privind diferențele de percepție și înțelegere a conceptelor tehnice, interesele subiective, diversitatea și imperfecțiunea legislativă, contextele de aplicare, etc.

Pentru responsabilii cu implementarea securității cibernetice este lipsit de sens să nu fie implementată varianta tehnică corectă a arhitecturilor și măsurilor de securitate cibernetică. De exemplu, pare absurd ca factorii decizionali să desconsidere argumentațiile tehnice și să implementeze doar parțial (sau deloc, uneori) viziunea de securitate cibernetică; ori ca managementul să nu înțeleagă principalele necesități de securitate cibernetică, chiar și în urma producerii frecvente a unor incidente de securitate.

Pentru aplicarea corectă a măsurilor de securitate cibernetică avem nevoie de colaborare continuă și de completare reciprocă a eforturilor, avem nevoie să depășim orgoliile concurențiale, întrucât riscurile cibernetice ridică probleme existențiale, de supraviețuire a business-urilor și oricine gândește și acționează singular se izolează, devenind o victimă sigură a incidentelor cibernetice. Securitatea cibernetică are nevoie de comandă și control unice, care să asigure prevenție și răspuns la incidentele cibernetice în timp real, precum și răspundere asumată asupra desfășurării evenimentelor și care să se sincronizeze cu alți omologi, responsabili de buna funcționare și de administrarea tehnologiei.

În viitor, asigurarea serviciilor de tehnologie (IT&C și OT) și a serviciilor de securitate cibernetică va fi o necesitate imperativă, fundamentală. În plus față de achiziția, motivația și retenția de personal specializat, organizațiile trebuie să aloce fonduri pentru investiții în echipamente și în servicii de administrare, mentenanță și suport al acestora.

Fie că sunt dezvoltate in-house sau externalizate, administrarea și asigurarea securității și apărării cibernetice solicită eforturi financiare proporționale cu necesitățile specificului obiectului muncii (misiunea organizației) și a rezultatelor evaluărilor de risc. În lipsa alocării de fonduri, nivelul de performanță funcțională scade, iar expunerea la riscuri crește, deschizând calea spre stagnare, sau chiar pierdere a business-ului.

Este important de înțeles că asigurarea securității și apărării cibernetice nu este un efort punctual, pe care îl depunem o dată și ne servește pe termen nedefinit, ci un efort continuu, susținut, care necesită adaptare și creștere permanentă. Organizațiile trebuie să manifeste deschidere, să conștientizeze și să înțeleagă fenomenul evoluției tehnologice și al nevoilor de securitate cibernetică, alocând mereu resursele cuvenite, pentru a-și asigura compatibilitatea și dimensionarea în raport cu tendințele societății și funcționarea în condiții de performanță.

Concluzie

Securitatea și apărarea cibernetică eficiente încep cu o cultură și o echipă de securitate puternice și sunt cel mai bine susținute de politici de securitate, proceduri, instruiri și teste de securitate adecvate, frecvente. De aici trebuie început întotdeauna. Este important să aveți oameni cu abilități tehnice în echipa de securitate, dar toate abilitățile din lume sunt inutile fără atitudinea și cultura potrivită care să le susțină utilizarea corectă. Cultura de securitate a companiei dumneavoastră este modul în care toată lumea din organizație se comportă în raport cu securitatea și apărarea cibernetică. Este un proces. Toate

controalele de securitate sunt inutile, dacă sunt ignorate. Ele trebuie adoptate și utilizate. (Sfatul meu pentru a promova o cultură puternică de securitate este să desfășurați cursuri de securitate cibernetică frecvente în organizația dvs., pentru toți angajații. Cursuri distractive și captivante, cu accent deosebit pe instruirea personalului pentru a rezista ingineriei sociale, cum ar fi phishing- ul și malware-ul).

Referințe bibliografice

1. Cyber threat hunting. https://en.wikipedia.org/wiki/Cyber_threat_hunting
2. On premises software. https://en.wikipedia.org/wiki/On-premises_software
3. Secure by design. https://en.wikipedia.org/wiki/Secure_by_design
4. Softwarw defined perimeter. https://en.wikipedia.org/wiki/Software-defined_perimeter
5. Zero trust security model. https://en.wikipedia.org/wiki/Zero_trust_security_model

Accesul la informație vs protecția datelor cu caracter personal

Sergiu BOZIANU

Expert național în domeniul protecției datelor cu caracter personal

La data de 10.01.2022, au intrat în vigoare prevederile Legii nr. 175/2021 de modificare a unor acte normative (digitizarea), prin care au fost operate modificări la legislația din domeniul protecției datelor cu caracter personal care a avut următorul impact

Realitățile juridice de până la 10.01.2022

În anul 2012, odată cu intrarea în vigoare a Legii nr. 133/2011 privind protecția datelor cu caracter personal care a transpus Directiva 95/46/CE, au fost operate modificări la art. 8 din Legea nr. 982/2000 privind accesul la informație, prin care s-a indicat că accesul la datele cu caracter personal este efectuat în conformitate cu legislația privind protecția datelor cu caracter personal.

La rândul său, Legea nr. 133/2011 la art. 10 (în vigoare și în prezent) a stabilit expres că atunci când datele cu caracter personal sunt necesare în scopuri jurnalistice, prin derogare de la art. 5, 6 și 8 dom această lege, acestea pot fi prelucrate (colectate, stocate, utilizate, publicate) dacă datele se referă la persoane publice sau la faptele publice în care sunt implicate persoanele, în condițiile Legii nr. 64/2010 cu privire la libertatea de exprimare. Mai simplu spus, aceste derogări permit jurnaliștilor de a avea acces la datele cu caracter personal fără acordul persoanei sau de alte temeiuri legale care în mod ordinar (în alte cazuri decât scopurile statistice) operatorii de date trebuie să dispună (spre exemplu, pentru a avea temei legal pentru a accesa datele: procuratura trebuie să aibă pornită urmărirea penală, instanța de judecată trebuie să aibă o cerere pusă pe rol, banca trebuie să aibă o cerere de creditare în procedură etc.)

Suplimentar, Legea nr. 133/2011 la art. 23, stabilea că orice persoană fizică sau juridică (inclusiv ONG, autoritățile publice sau orice organizație) care dorea să prelucreze date (inclusiv mass-media sau orice altă persoană fizică sau juridică), era obligată să primească autorizația de la Centrul Național pentru Protecția Datelor cu Caracter Personal. Autorizarea era o procedură absolut birocratică,

or, până la finele anului 2021, s-au înregistrat circa 3000 operatori de date din cele peste 3 milioane de cereri depus.

În anul 2015, CNPDCP a emis decizia prin care a interzis ÎS,,CRIS,,Registru" de a oferi acces la bazele de date către persoanele care nu erau autorizate de CNPDCP http://old.datepersonale.md/file/decizii%20centrus/decizia.pdf

În 2018 au intrat în vigoare prevederile Legii nr. 142 cu privire la schimbul de date și interoperabilitate, prin care autoritățile publice au fost obligate să realizeze schimbul de date, inclusiv accesul la sursele de date exclusiv prin intermediul platformei guvernamentale, iar responsabili de autorizarea accesului la date fiind: Agenția de Guvernare electronică și CNPDCP.

Accesul la registrele de stat prin intermediul platformei de interoperabilitate se acorda de către AGE doar celor care dețineau autorizația din partea CNPDCP (obținerea autorizației putea dura 6 luni – 1 an) – circumstanțe care în mod nejustificat bloca consumul de date, fluxurile de date, procesele economice, activitatea de antreprenor, activitatea jurnalistică etc.

Realitățile juridice de după 10.01.2022

Prin Legea nr. 175/2021, a fost anulată procedura de înregistrare și autorizare în calitate de operator de date cu caracter personal, CNPDCP fiind-ui exclusă competența de autorizarea accesului la platforma de interoperabilitate, AGE păstrându-și în acest sens competența deplină a acordarea accesului la registrele de stat.

Prevederile art. 10 din Legea nr. 133/2011 privind protecția datelor cu caracter personal au rămas aplicabile și în continuare.

Astfel, prin Legea nr. 175/2021, au fost excluse aspectele birocratice privind obținerea autorizației din partea CNPDCP, ameliorându-se premisele pentru obținerea accesul la informație inclusiv la datele cu caracter personal de interes public, aspecte reflectat și în presă http://old.media-azi.md/ro/stiri/anularea-obliga%C8%9Biei-de-%C3%AEnregistrare-ca-operator-de-date-cu-caracter-personal-%C8%99i-beneficiile

Mai mult, măsurile administrative luate de ASP de după aceste modificări cu privire la obținerea accesului la informației doar în baza unor cereri scrise fără acordarea accesului la resursele informaționale de stat, nu are o legătură cu modificările operate prin Legea nr. 175/2021.

Femeia lider: obstacole și oportunități

Cine este femeia lider? În ciuda progreselor din ultimele decenii, femeile sunt încă subreprezentate în roluri de conducere în multe industrii și țări. Acest lucru se datorează unei varietăți de factori, inclusiv prejudecățile și discriminarea de gen, așteptările sociale și culturale cu privire la rolurile de gen. Lupta continuă a femeilor pentru a demonstra capacitatea sa de a fi lider societății este ca un adevărat flagel. Biasurile de gen și stereotipurile rămân o problemă în multe domenii, inclusiv în cibernetică și în alte domenii tehnologice, ceea ce poate duce la subestimarea sau ignorarea calităților și competențelor femeilor lider.

Daniela POPUȘOI

Facultatea Relații Internaționale, Științe Politice și Jurnalism, ULIM

Poziția de lider

Oamenii devin lideri prin interiorizarea unei identități de lider și dezvoltarea unui simț al scopului. Interiorizarea sentimentului de sine ca lider este un proces frecventativ. O persoană își afirmă conducerea prin acțiuni intenționate, cum ar fi convocarea unei întâlniri pentru a restarta un proiect latent. Alții afirmă sau rezistă acțiunii, încurajând sau descurajând astfel afirmațiile ulterioare. Aceste interacțiuni informează persoana asupra sentimentului de sine în calitate de lider și comunică modul în care alții văd capacitatea sa pentru acest rol.

A deveni lider implică mult mai mult decât a fi pus într-un rol de conducere, dobândirea de noi abilități și adaptarea stilului cuiva la cerințele acelui rol. Ea implică o schimbare fundamentală de identitate. A deveni lider implică un simț clar al scopului, o dorință de a-și asuma responsabilitatea și capacitatea de a inspira și influența pe alții să lucreze la o viziune comună.Un lider este cineva care inspiră, motivează și dă putere altora să lucreze împreună pentru a realiza o viziune comună. A fi lider înseamnă a-și asuma responsabilitatea pentru un grup de oameni și a-i ghida către un obiectiv comun. Liderii sunt comunicatori eficienți și sunt capabili să transmită altora viziunea și obiectivele în mod clar și persuasiv. Liderii sunt capabili să ia decizii dificile în timp util și eficient, adesea sub un nivel ridicat de presiune. Liderii sunt capabili să își ajusteze abordarea în funcție de circumstanțe în schimbare și sunt dispuși să-și asume riscuri pentru a-și atinge obiectivele. Liderii își asumă responsabilitatea pentru acțiunile lor și

a celor pe care îi conduc și sunt dispuși să învețe din greșelile lor. Dar ce implică acțiunea de a deveni și de a fi lider pentru o femeie? În ciuda progreselor din ultimele decenii, femeile sunt încă subreprezentate în roluri de conducere în multe industrii și țări. Acest lucru se datorează unei varietăți de factori, inclusiv prejudecățile și discriminarea de gen, așteptările sociale și culturale cu privire la rolurile de gen.

Dacă facem o paranteză din punct de vedere istoric, vedem cum discriminarea de gen se devalorifică tot mai mult datorită mișcărilor feministe. La sfârșitul secolului al XIX-lea și începutul secolului al XX-lea, femeile din multe țări au luptat pentru dreptul de vot și de a participa la procesul politic. Mișcarea votului a reprezentat un pas esențial către o mai mare reprezentare politică a femeilor și a ajutat la a pune bazele altor mișcări feministe. În anii 1960 și 1970, a apărut un nou val de feminism care s-a concentrat pe probleme precum drepturile reproductive, egalitatea de remunerare și eradicarea violenței bazate pe gen. Această mișcare a contribuit la creșterea gradului de conștientizare cu privire la modurile în care femeile sunt încă discriminate și a contribuit la realizarea unor schimbări legale și sociale importante.Mai recent, mișcarea feministă a devenit mai incluzivă și intersecțională, recunoscând că femeile se confruntă cu discriminarea și inegalitatea bazate pe factori precum rasa, sexualitatea și statutul socioeconomic. Acest lucru a condus la o abordare mai nuanțată și incluzivă a feminismului, care încearcă să abordeze experiențele tuturor femeilor. Caracterul incluziv al feminismului, a reușit să cuprindă practic toate ramurile ce reprezentau insustenabilitate pentru dezvoltarea și promovarea imaginii femeilor în domenii precum economie, politică, cibernetică, etc. La etapa actuală femeile încă întâlnesc dificultăți în aspecte cum ar fi rolul lor în societate și mai ales necesitatea acestora în pozițiile de lider.

Femeia lider pentru societate

Femeile încă se confruntă cu discriminare și părtinire în multe aspecte ale vieții lor, de la deciziile de angajare și promovare până la atitudinile culturale cu privire la abilitățile și rolurile femeilor în societate.Pentru o femeie, în procesul de ascensiune către un rol de lider va fi nevoie de dovezi aduse constant că aceasta este sau nu capabilă să gestioneze domeniul. Această plauzibilitate a muncii și eforturilor sale a devenit un obiectiv ascuns la nivel de subconștient, fie a femeii către sine, fie a femeii către societate. Pentru societate, femeia lider este „o doamnă de fier" caresugerează că o femeie lider este rece, aspră și nemiloasă, concentrându-se adesea pe putere și control asupra compasiunii și empatiei (exemplul bine cunoscut al fostei prim-ministre al Marii Britanii,

Margaret Tatcher). Pentru societate, femeia lider este „femeie cu copii", aici ne referim la stereotipul denumit pedeapsa maternității- fenomen în care femeile sunt penalizate în carieră pentru că au copii sau sunt percepute ca îngrijitoare. Se presupune adesea că femeile care au copii vor fi mai puțin angajate în cariera lor sau vor fi mai puțin competente decât omologii lor bărbați care au familii. Această părtinire poate fi întărită de normele culturale și instituționale care acordă prioritate muncii bărbaților și avansării în carieră față de cea a femeilor. Un alt clișe pus de societate se bazează pe simpatie, când femeile lideri sunt așteptate să fie simpatice și plăcute, în timp ce bărbații pot fi aserți și încrezători fără a se confrunta cu aceleași așteptări. Acest lucru poate duce la prejudecăți împotriva femeilor lideri care sunt considerate prea asertive sau nu suficient de simpatice. Deci, deși am atins unele standarte în aspectul egalității de gen, o femeie lider va fi nevoită să se lupte constant cu stereotipurile impuse, intenționat sau neintenționat , de către societate și mediul său de activitate. Organizațiile amplifică ,din neatenție, acest proces atunci când sfătuiesc femeile să caute în mod proactiv, roluri de conducere fără a aborda și politicile și practicile care comunică o nepotrivire între modul în care sunt văzute femeile și calitățile și experiențele pe care oamenii tind să le asocieze cu liderii.Nu este suficient să identifici și să insufli abilitățile și competențele „potrivite" ca într-un vid social. Contextul trebuie să susțină motivația unei femei de a conduce și, de asemenea, să crească probabilitatea ca alții să recunoască și să încurajeze eforturile ei, chiar și atunci când ea nu arată sau nu se comportă ca reprezentanții funcțiilor înalte deja ocupate.

Femeile pot fi lideri extrem de eficienți, la fel ca bărbații. Nu există niciun motiv inerent pentru care femeile nu pot avea succes în poziții de conducere și, de fapt, există numeroase exemple de femei care au excelat ca lideri în diverse domenii. Femei a căror domenii de activitate și realizări inspiră și ajută la motivarea fiecărui din noi, femei și inclusiv a bărbaților. Un exemplu potrivit ar fi Eleanor Roosevelt. Eleanor Roosevelt a fost o campioană a drepturilor femeilor și a crezut cu tărie în potențialul femeilor ca lideri. În calitate de soție a președintelui Franklin D. Roosevelt, și-a folosit poziția pentru a susține problemele femeilor și pentru a promova oportunități pentru femei în politică și în forța de muncă. În timpul președinției soțului ei, Eleanor a ținut periodic conferințe de presă pentru reportere și a susținut politicile care promovau egalitatea de gen. Ea a fost, de asemenea, președinte a Comisiei președintelui privind statutul femeii în anii 1960, care a fost însărcinată cu examinarea statutului femeilor în societatea americană și să facă recomandări pentru a-și îmbunătăți oportunitățile și bunăstarea.Pe lângă munca ei în politică, Eleanor a fost o puternică susținătoare a educației și credea că femeile ar trebui să aibă acces la aceleași oportunități

educaționale ca și bărbații. De asemenea, ea a încurajat femeile să-și dezvolte abilitățile de conducere și să-și folosească vocile pentru a susține schimbarea socială și politică.

Dăruirea neclintită a lui Eleanor Roosevelt pentru justiția socială, conducerea și rezistența ei în fața adversității și angajamentul ei față de educație și serviciul public fac din ea o figură inspiratoare și un exemplu minunat de urmat.

Femeile aduc adesea un set unic de abilități și perspective la locul de muncă, inclusiv empatie, intuiție, creativitate și un stil de comunicare diferit, care pot ajuta la construirea de echipe mai puternice și la rezolvarea problemelor într-un mod mai inovator.Totuși, femeile încă se confruntă cu obstacole în ceea ce privește accesul la poziții de conducere și la oportunități de avansare în carieră. Biasurile de gen și stereotipurile rămân o problemă în multe domenii, inclusiv în cibernetică și în alte domenii tehnologice, ceea ce poate duce la subestimarea sau ignorarea calităților și competențelor femeilor lider. În cele din urmă, este important să se recunoască că calitățile de lider sunt mai importante decât sexul sau genul. Atât femeile, cât și bărbații pot fi lideri eficienți, iar valorizarea diversității și a incluziunii în organizații poate duce la echipe mai puternice și mai bune.

Femeia lider în securitatea cibernetică

În general, subreprezentarea femeilor în domenii precum: inginerie, tehnologii informaționale, știință ș.a. este o problemă complexă care e influențată de o varietate de factori, inclusiv stereotipuri și părtiniri de gen, norme culturale și societale și bariere instituționale. Eforturile de abordare a acestor probleme pot include inițiative care vizează reducerea prejudecăților și stereotipurilor de gen, creșterea accesului la educație și formare și promovarea politicilor care susțin echilibrul dintre viața profesională și viața privată și egalitatea de gen la locul de muncă.

Domeniul ciberneticii este un domeniu și mai specific la capitotul incluziunea femeilor.Femeile au fost subreprezentate istoric în domeniul securității cibernetice și continuă să se confrunte cu provocări semnificative în această industrie dominată de bărbați. Cu toate acestea, există multe femei care aduc contribuții importante în domeniu și lucrează pentru a depăși barierele din calea egalității de gen.Unele dintre provocările cu care se confruntă femeile din domeniul cibernetic includ:

a. Prejudecățile și discriminarea de gen: femeile din securitatea cibernetică se confruntă adesea cu părtiniri și discriminare, atât în ceea ce privește deciziile de angajare și promovare, cât și în interacțiunile lor zilnice cu colegii și clienții.

b. Lipsa modelelor feminine: există relativ puține modele feminine în securitatea cibernetică, ceea ce poate face dificil pentru femei să se vadă ca aparținând domeniului și le poate limita oportunitățile de mentorat și sprijin.

c. Salariu inegal și oportunități de promovare: femeile din securitatea cibernetică câștigă adesea mai puțin decât omologii lor de sex masculin și se pot confrunta cu mai puține oportunități de promovare și avansare în carieră.

În ciuda acestor provocări, există multe femei care aduc contribuții semnificative în domeniul securității cibernetice și lucrează pentru a promova o mai mare egalitate de gen. Femeile conduc proiecte inovatoare, dezvoltă noi tehnologii și pledează pentru o mai mare diversitate și incluziune în industrie.Organizații precum Women in Cybersecurity (WiCyS) și International Consortium of Minority Cybersecurity Professionals (ICMCP) lucrează pentru a sprijini femeile și alte grupuri subreprezentate în domeniu și pentru a promova o mai mare diversitate și incluziune în securitatea cibernetică. În general, participarea și conducerea femeilor în securitatea cibernetică este esențială pentru a aborda deficitul de forță de muncă din industrie și pentru a asigura că domeniul este mai reprezentativ pentru diversele comunități pe care le deservește.

Putem să urmărim și exemple notabile printre femeile care sunt lideri de succes în domeniul securității cibernetice, de exemplu:Dr. Fei-Fei Li, un lider în domeniul inteligenței artificiale și al învățării automate, fostă profesoară la Universitatea Stanford și a condus Google Cloud AI, iar acum este fondatoarea și CEO-ul companiei de start-up AI4ALL; Debora Plunkett, fosta directoare al National Security Agency (NSA) și a jucat un rol important în dezvoltarea și implementarea unor programe de securitate cibernetică de vârf la nivel național și sigur că Shafi Goldwasser- pionieră în criptografia modernă și în teoria complexității computaționale, câștigând premiul Turing, cel mai prestigios premiu în informatică, în 2012. Toate aceste femei au reușit să progreseze în acest domeniu datorită abilităților și cunoștințelor lor în domeniu și gestionarea lor pentru a deveni lideri ai segmentului.

Calitățile unei femei lider în securitate cibernetică sunt similare cu cele ale oricărui alt lider, dar pot include și unele calități unice care pot ajuta femeile să reușească în acest domeniu dominat de bărbați. Unele dintre aceste calități includ

expertiză tehnică.Expertiza tehnică este bază solidă în conceptele de securitate cibernetică și abilitățile tehnice este esențială pentru succesul în acest domeniu. Femeile lideri în domeniul securității cibernetice ar trebui să aibă o înțelegere profundă a tehnologiilor de securitate, a amenințărilor și vulnerabilităților și a tendințelor din industrie. Nu putem exclude nici abilitățile de comunicare. Comunicarea este esențială pentru succesul conducerii în orice domeniu, dar este deosebit de importantă în securitatea cibernetică, unde jargonul tehnic și conceptele complexe pot fi greu de înțeles. Femeile lideri în domeniul securității cibernetice ar trebui să poată comunica clar și eficient cu părțile interesate atât tehnice, cât și non-tehnice. Pentru un lider femeie, abilitățile sale de conducere sunt mail mult decât necesare. Leadership-ul este esențial pentru succesul în orice domeniu, iar femeile lider în securitate cibernetică ar trebui să fie capabile să inspire, să motiveze și să gestioneze eficient echipele. De asemenea, ar trebui să fie capabili să conducă prin exemplul, dând un ton pozitiv și creând o cultură a incluziunii și a diversității. Și nu în ultimul rând, reziliența. Securitatea cibernetică poate fi un mediu de mare presiune și stres ridicat, iar liderii de sex feminin în securitate cibernetică ar trebui să fie capabili să-și mențină calmul și rezistența în fața provocărilor și eșecurilor.

Acestea sunt doar câteva dintre calitățile care sunt importante pentru femeile lider în securitatea cibernetică. Femeile care posedă aceste calități și care sunt dispuse să muncească din greu și să persevereze în fața adversității, pot obține un mare succes în acest domeniu provocator și plin de satisfacții.

Concluzie

Leadershipul se referă la capacitatea de a inspira, motiva și ghida pe alții către un scop sau o viziune comună, indiferent de sex. Există numeroase exemple de lideri eficienți de toate genurile de-a lungul istoriei și în diverse domenii, inclusiv politică, afaceri și activism social. Trăsăturile și abilitățile care fac un lider grozav, cum ar fi empatia, comunicarea, gândirea strategică și luarea deciziilor, nu sunt exclusive pentru un anumit gen. De fapt, promovarea diversității și a incluziunii în conducere este crucială pentru crearea unei societăți mai echitabile și mai justă. Prin recunoașterea și prețuirea contribuțiilor tuturor indivizilor, indiferent de sexul lor, putem accesa o gamă mai largă de perspective și experiențe, care în cele din urmă pot duce la luarea deciziilor și la rezultate mai bune. Putem promova diversitatea și incluziunea în leadership prin crearea unei culturi a incluziunii. Liderii pot promova diversitatea și incluziunea prin crearea unei culturi a incluziunii în organizațiile lor. Acestea pot include politici care asigură egalitatea de șanse și un sentiment de apartenență pentru toți angajații,

indiferent de trecutul sau identitatea acestora. Prin promovarea diversității și incluziunii în leadership, organizațiile pot beneficia de o gamă mai largă de perspective și experiențe, ceea ce poate duce la o mai bună luare a deciziilor, la îmbunătățirea creativității și a inovației și la creșterea angajamentului și a satisfacției angajaților.

Dacă e să vorbim despre femeia lider, acestea au adesea abilități și trăsături de liderat care sunt valoroase pentru o varietate de situații și domenii. Aceste abilități pot include, printre altele, abilități de comunicare, empatie, adaptabilitate, gândire strategică, luare a deciziilor, curaj și încredere. Femeile lideri pot aduce o perspectivă diferită asupra situațiilor, datorită experiențelor și perspectivelor lor unice. De exemplu, o femeie lider care a înfruntat discriminarea sau inegalitatea poate fi mai motivată să promoveze diversitatea și echitatea în organizație. Există numeroase exemple de femei lideri care au condus cu succes organizații dintr-o varietate de domenii, de la afaceri la politică și la activități sociale. Aceste femei lideri au reușit să obțină rezultate semnificative, cum ar fi creșterea veniturilor, îmbunătățirea proceselor și creșterea impactului social. Promovarea egalității de gen în leadership poate contribui la creșterea diversității și a incluziunii în organizații, ceea ce poate conduce la creșterea productivității și a creativității și la îmbunătățirea satisfacției angajaților. Femeile au fost subreprezentate în domeniul tehnologiei și al securității cibernetice, dar există multe femei care lucrează în acest domeniu și care dețin funcții de conducere. Acestea sunt adesea capabile să abordeze provocările de securitate cibernetică printr-o abordare multidisciplinară, prin folosirea abilităților lor de comunicare, de gestionare a riscurilor și de gândire strategică. De exemplu, femeile lider din securitatea cibernetică pot fi mai orientate către securitatea utilizatorilor și pot fi mai atente la necesitatea de a construi un mediu de lucru echilibrat și sigur pentru echipele de tehnologie. De asemenea, femeile lider pot fi mai atente la echilibrul dintre securitatea și intimitatea datelor și la nevoia de a proteja drepturile utilizatorilor în timp ce se asigură că datele sunt protejate. Este important să se promoveze diversitatea în securitatea cibernetică pentru a aborda o varietate de amenințări și a dezvolta soluții mai eficiente. Prin promovarea femeilor lider în domeniul securității cibernetice, putem aduce abordări noi și inovatoare pentru a aborda amenințările cibernetice în continuă evoluție și pentru a construi un mediu de lucru mai divers și mai echitabil.

Referințe bibliografice

1. Y.Keim, Running a WiCyS Chapter — tips, tricks, secrets and perks!, 2019. https://www.wicys.org/running-a-wicys-chapter-tips-tricks-secrets-and-perks/
2. H. Ibarra, J. Ely, D. Kolb, Women Rising: The Unseen Barriers, 2013. https://hbr.org/2013/09/women-rising-the-unseen-barriers
3. Women Deliver community, Women in Leadership, 2019. https://womendeliver.org/womensleadership/
4. Cybersecurity Ventures, Women in cybersecurity report, 2022. https://cybersecurityventures.com/wp-content/uploads/2022/09/Women-In-Cybersecurity-2022-Report-Final.pdf
5. S. Morgan,Women Hold 25 Percent Of Cybersecurity Jobs Globally In 2022.2022 https://cybersecurityventures.com/women-in-cybersecurity-report-2022/

Importanța securității cibernetice a Republicii Moldova în contextul războiului hibrid purtat de Federația Rusă

Mihaela MELNIC

Biblioteca Municipală "B.P. Hasdeu"

De la anexarea Crimeii în anul 2014, expresia „război hibrid" este tot mai frecvent întâlnită și folosită pentru a descrie "o interacțiune dinamică între elemente de tip hard power (consolidarea forțelor militare, dispunerea de forțe și capabilități militare în zone de conflict, finanțarea unor mișcări separatiste, activități de destabilizare și subminare a securității unui stat sau regiuni) și elemente de tip soft power (menținerea unei dependențe economice sau energetice, sancțiuni economice aplicate, campanii de propagandă, dezinformare, influențare și atacuri cibernetice)"[1]. Organizarea atacurilor cibernetice asupra unor actori statali pentru atingerea obiectivelor de politică externă a devenit o practică obișnuită a războiului hibrid din ultimii ani. Federația Rusă se numără printre statele care au dezvoltat o strategie sofisticată în acest sens, transformând spațiul cybernetic într-un domeniu operațional împotriva statelor pe care încearcă să le influențeze, să le știrbească din suveranitate și integritate sau să le destabilizeze.

Prima operațiune cibernetică motivată politic și sponsorizată de stat, cunoscută în istorie, este agresiunea cibernetică a Rusiei asupra Estoniei din anul 2007. Aceasta a constituit o acțiune punitivă a Rusiei în urma deciziei autorităților estoniene de a reloca memorialul sovietic al "Soldatului de Bronz" din central Tallinnului. Timp de 3 săptămâni, atacurile cibernetice de tip DDoS (Distributed Denial of Service) au paralizat infrastructura digital a Estoniei și au cauzat indisponibilitatea serverelor guvernamentale, ale agențiilor de presă, furnizorilor de servicii de internet, băncilor importante și întreprinderilor mici. Situația a fost exploatată de partea rusă prin susținerea acțiunilor de protest atât în Estonia, cât și la Moscova, în fața ambasadei estoniene, dar și mediatic, prin prezentarea incidentului ca fiind un atac la adresa memoriei soldaților sovietici căzuți la datorie și prin insinuarea de simpatii naziste autorităților estoniene[2]. Atacul cibernetic asupra Estoniei din 2007 poate fi considerat un exemplu elocvent despre cum o țară poate fi paralizată prin atacuri cibernetice, iar nemulțumirile

populare– exploatate și amplificate pe fundalul acestui blocaj. Un an mai târziu, hackerii ruși au organizat un atac DDoS asupra Georgiei, blocând accesul la internet înainte ca trupele rusești să invadeze țara. Același scenario Rusia a încercat să aplice și în februarie 2022, când a pregătit invadarea Ucrainei. Prin urmare, Rusia este un exemplu tipic de țară care adoptă un comportament hard în spațiul cibernetic.

Odată cu declanșarea războiului din Ucraina, Republica Moldova a resimțit la maximum efectele războiului hybrid desfășurat de Federația Rusă, inclusiv pe partea de securitate cibernetică, unde s-a atestat o creștere fără precedent a numărului, intensității și complexității atacurilor cibernetice. Într-un interviu acordat pentru Euronews, cu ocazia deplasării la Bruxelles pentru un summit UE-Moldova, prim-ministra Republicii Moldova Natalia Gavriliță descrie folosirea atacurilor cibernetice drept unul dintre elementele războiului hibrid purtat de Rusia în Republica Moldova prin care se încearcă destabilizarea țării noastre. Potrivit prim-ministrei, în anul 2022 a fost înregistrat cel mai mare număr de atacuri cibernetice din istoria țării noastre[3]. Anul trecut, pentru prima data, a fost posibilă atribuirea atacurilor Rusiei, operațiunea fiind desfășurată de gruparea pro-rusă Killnet cea activează pe principii de hacktivism. Prin atacuri de tip DDoS, hacktiviștii pro-ruși au vizat site-urile instituțiilor de stat din Republica Moldova și au avut drept scop blocarea paginilor web prin transmiterea unui număr mare de cereri de conexiune sau a unui volum mare de date, suprasolicitând resursele de procesare ale echipamentelor și cauzând indisponibilizarea paginilor web. Atacurile au fost efectuate de pe echipamente și rețele compromise situate în afara teritoriului Republicii Moldova, prin exploatarea unor vulnerabilități de securitate și înrolarea acestora în rețelele botnet[4]. Pe 23 august 2022, hackerii de la Killnet au amenințat că vor ca reţelele instituţiilor din Republica Moldova, publicând pe rețelele de socializare următorul mesaj: „Să înceapă iadul pe pământul Moldovei. Ping-ul rețelei de stat se va opri săptămâni întregi, iar apoi cu siguranță vor conștientiza totul în lacrimi...”[5]. Urmare a acestor amenințări, Republica Moldova a contracarat în următoarele 72 de ore peste 80 de atacuri cibernetice împotriva sistemelor sale informatice, platformelor şi portalurilor publice strategice, conform unui comunicat al Serviciului Tehnologia Informaţiei şi Securitate Cibernetică (STISC) din data de 25 august 2022[6].

În ceea ce privește dinamica operațiunii cibernetice împotriva Republicii Moldova, conform viceprim-ministrului pentru digitalizare Iurie Țurcanu, atacurile “au început în luna martie după invazia rusă în Ucraina și au continuat pe parcursul anului 2022, iar cele mai mari atacuri cibernetice au fost înregistrate în lunile mai și august”[7]. Aceste tendințe ne arată că Federația Rusă desfășoară o operațiune cibernetică susținută împotriva țării noastre, cu un risc constant de intensificare. În aceste circumstanțe, pentru Republica Moldova, este esențială

abordarea securității cibernetice drept o prioritate a securității naționale, precum și consolidarea capacităților de apărare cibernetică.

Importanța securității cybernetic este dictată de însăși caracterul specific al operațiunilor cibernetice, adică de diferența majoră dintre o operațiune militară și o operațiune cibernetică care constă în faptul că ultima nu ține de proximitatea fizică și poate fi privită ca o modalitate de a purta un război fără limitări teritoriale și a ținti orice sector al securității naționale din orice colț al lumii. Printr-o singură operațiune cibernetică, atacatorul poate bloca un sector de activitate vital al țării agresate. De exemplu, eșecul de a anticipa și contracara un atac asupra unei rețele publice de telecomunicații ar putea lăsa clienții fără serviciul telefonic. Daune financiare considerabile pot rezulta în urma atacurilor împotriva sistemului bancar, finanțelor și comerțului. Țintirea sistemelor informatice ale serviciului vamal poate duce la blocarea traficului transfrontalier și formarea cozilor.Unele atacuri cibernetice pot avea un impact considerabil asupra funcționării normale a societății, cu consecințe neprevăzute și potențial dezastruoase. Acestea se pot produce ca urmare a țintirii infrastructurii critice și a sistemelor informatice associate acesteia. Un atac cibernetic îndreptat împotriva sistemelor de control ale unei instalații chimice sau de gaze natural ar putea duce la consecințe fizice considerabile și chiar la pierderi de vieți omenești. Printre cele mai grave scenarii de amenințare, totuși, se numără cele care implică o combinație de atacuri cibernetice și atacuri fizice sau atacuri cibernetice lansate în timpul unui dezastru natural major[8].

Pentru a face față amenințărilor hibride și a asigura un nivel înalt de securitate cibernetică, Republica Moldova are nevoie de o reglementare a domeniului securității cibernetice și o abordare de management centralizată. În acest sens, este primordial adoptarea Legii și Strategiei privind securitatea cibernetică, precum și înființarea unui Centru de răspuns la incidente de securitate cibernetică (CERT) la nivel național. De asemenea, aceste măsuri trebuie suplinite de investiții în pregătirea de specialiști calificați, acțiuni de conștientizare și educare a unei culturi de igienă cibernetică în rândul populației, dotarea cu echipamente și software, cooperare internațională și schimb de bune practici.

În condițiile în care Republica Moldova se află în plin război informațional, iar atacurile cibernetice au devenit tot mai frecvente şi mai complexe, asigurarea unei securități cibernetice înalte este crucial pentru securitatea națională, în special, în contextul în care spațiul cibernetic constituie unul dintre instrumentele de bază în desfășurarea războiului hibrid. Așadar, pentru Republica Moldova, securitatea cibernetică contează cu atât mai mult cu cât mediul virtual este un câmp de luptă major împotriva acțiunilor agresive și subversive ale Federației Ruse.

Referințe bibliografice

1. Iordan Oana. 2017. Război hybrid şi atacuri cibernetice. https://intelligence.sri.ro/razboi-hibrid-si-atacuri-cibernetice/ (accesat 12.02.2023).
2. Budnitsky Stanislav. 2022. A Relational Approach to Digital Sovereignty: e-Estonia Between Russia and the West". In: International Journal of Communication 16 (2022): p.1918–1939.
3. Koutsokosta Efi. Russia conducting 'hybrid war' in Moldova with protests andcyber attacks: Prime Minister". https://www.euronews.com/my-europe/2023/02/07/russia-conducting-hybrid-war-in-moldova-with-protests-and-cyber-attacks-prime-minister (accesat 09.02.2023).
4. Andone Radu. 2022. Zeci de atacuri cibernetice în Republica Moldova. Au fost vizate portalurile publice"., https://www.capital.ro/zeci-de-atacuri-cibernetice-in-republica-moldova-au-fost-vizate-portalurile-publice.html (accesat 12.02.2023).
5. Laur Victoria. Să vină iadul pe pământul Moldovei. Hackerii ruși anunță atacuri de o săptămână asupra instituțiilor noastre". https://realitatea.md/sa-vina-iadul-pe-pamantul-moldovei-hackerii-rusi-anunta-atacuri-de-o-saptamani-asupra-institutiilor-noastre/ (accesat 12.02.2023).
6. Comunicat informative privind tentativele de atac cibernetic din ultimele 72 de ore". 25 https://stisc.gov.md/ro/comunicat-informativ-privind-tentativele-de-atac-cibernetic-din-ultimele-72-de-ore (accesat 12.02.2023).
7. Cel mai mare val de atacuri cibernetice din istoria Republicii Moldova a avut loc în 2022". https://noi.md/md/societate/cel-mai-mare-val-de-atacuri-cibernetice-din-istoria-republicii-moldova-a-avut-loc-in-2022 (accesat 09.02.2023).
8. Ministerul Apărării din Estonia. 2008. Strategia de Securitate Cibernetică. Tallinn, Comitetul pentru Strategia de Securitate Cibernetică.

Identitatea online și consecințele acesteia asupra drepturilor omului

Mihaela BÎRLIBA

BC "MAIB" S.A."

Într-o lume în care noi suntem conectați la rețeaua globală internet, utilizând pe larg serviciile online, dobândim o nouă identitate și anume identitatea online sau identitatea digitală. Identitatea online se constituie dintr-un set de date, informații, caracteristici ale persoanei fizice pe care noi le lăsăm în mediul online, fie că o facem în mod voluntar sau fără să știm acest lucru. Identitatea digitală este generată de activitatea noastră în mediul online.

Persoana fizică conștient își construiește o identitate digitală prin crearea diferitor conturi pe rețele de socializare și publicarea informațiilor personale – poze, date de identificare – nume, prenume, data, luna, anul nașterii ș.a., precum și prin like-urile pe care le dăm la diferite postări în mediul online, comentarii, sau diferitele pagini, profiluri accesate sau acceptând anumiți termeni și condiții atunci când accesăm diferite pagini web, inclusiv fișierele de tip cookies care colectează despre noi foarte multe informații.

Identitatea digitală include și acele date pe care noi deși nu le indicăm sau oferim direct, acestea sunt colectate și anume: activitățile de căutare online, istoricul cumpărăturilor online, adresa IP, date ce țin de dispozitivul nostru - modelul, sistem de operare, anumite preferințe la accesarea diferitor site-uri, limba, geolocația ș.a.

Ulterior toate aceste informații sunt utilizate în scop de profilare. Dar ce este profilarea?

Profilarea reprezintă combinarea mai multor metode de prelucrare automată a datelor personale ale persoanei fizice "lasate" în mediul online care constau în utilizarea acestor date pentru a evalua anumite aspecte ce țin de o persoană, în special pentru a analiza, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică sau deplasările acesteia etc.

Aceste date colectate sunt utilizate în diferite scopuri de către diferite instituții

publice sau private (numiți în continuare "operatori"), "pentru îmbunătățirea calității serviciilor sau experienței clientului" așa cum declară majoritatea operatorilor în politica de confidențialite, pentru afișarea unor oferte personalizate, trimiterea publicității, pentru a ne determina sau chiar influența preferințele, astfel încât produsele/serviciile/oportunitățile care ne sunt oferite să corespundă acestora și "să ne țintească" cât mai bine.

Prelucrarea automatizată a acestor profiluri este urmată de cele mai dese ori de emiterea unei decizii automate, adică luarea unor decizii cu ajutorul tehnologiei, fără intervenția factorului uman.Regulamentul european privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (în continuare "GDPR"), prevede că o persoană are dreptul să nu facă obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri și poate să-i ceară operatorului de date acest lucru[4].

Acest drept se regăsește și în Legea privind protecția datelor cu caracter personal, nr. 133/2011, care la art. 17 consacră dreptul de a nu fi supus unei decizii individuale, potrivit căruia: "[1] *Orice persoană are dreptul de a cere anularea, în totalitate sau parţială, a oricărei decizii individuale care produce efecte juridice asupra drepturilor şi libertăţilor sale, fiind întemeiată exclusiv pe prelucrarea automatizată a datelor cu caracter personal destinată să evalueze unele aspecte ale personalităţii sale, precum competenţa profesională, credibilitatea, comportamentul şi altele asemenea.*

(2) Persoana poate fi supusă deciziei prevăzute la alin.(1) în cazul în care:

a) decizia este autorizată de o lege care stabileşte măsurile ce garantează apărarea interesului legitim al subiectului datelor cu caracter personal;

b) decizia este luată în cadrul încheierii sau executării unui contract, cu condiţia că cererea de încheiere sau de executare a contractului depusă de subiectul datelor cu caracter personal a fost satisfăcută[3]"

Din textul de lege citat supra, deducem că avem dreptul să solicităm operatorului anularea totală sau parțială a deciziei emise în privința noastră prin utilizarea unor procese automatizate de analiză, dacă aceasta ne afectează drepturile noastre, iar un exemplu în acest sens ar fi evaluarea angajaților la locul de muncă prin diferite camere de supraveghere dotate cu sisteme de inteligență artificială, care în baza unor parametri setați, pot să evalueze cât de productivi suntem la locul de muncă, evaluarea fiind urmată de emiterea deciziilor de stimulare a angajaților sau din contra decizii de sancționare. Un exemplu este compania Uber, care a fost pe larg criticată pentru sistemul de evaluare a angajaților implementat, potrivit căruia șoferii de taxi primesc anumite note de la utilizatorii aplicației Uber, iar

șoferii care primesc note mai mici de 4.6 - nota maximă fiind 5, primesc refuz de a avea acces la serviciu, ceea ce implică afectarea semnificativă a drepturilor la muncă[5].

E normal să nu preferăm ca un algoritm să decidă ceva pentru noi, fără absolut nicio intervenție umană, dar trebuie să nu uităm și de acele excepții când operatorii sunt în drept să utilizeze procesele decizionale automatizate, și anume situația când decizia automatizată este autorizată prin legi speciale care au ca scop apărarea interesului legitim al persoanei vizate, sau al unui interes public major, atunci când în joc sunt puse sănătatea publică sau securitatea statului sau atunci când decizia este luată în procesul de încheiere sau executare a unui contract, inițiat la cererea persoanei vizate, cu condiția că această cerere a fost satisfăcută în mod favorabil pentru persoana vizată. Un exemplu relevant în acest sens reprezintă acele prelucrări automatizate făcute de bănci sau organizații de creditare nebancară atunci când se face acea analiză a bonității persoanei, acel "scoring", care în baza evaluării anumitor condiții de eligibilitate, decide acordarea creditului sau nu.

Operatorilor le revine sarcina, inclusiv obligația prin prisma GDPR de a explica clar și simplu persoanelor vizate modul în care funcționează crearea de profiluri și procesul decizional automatizat, iar informarea trebuie furnizată într-o formă pe înțelesul unei persoane fără cunoștințe tehnice, astfel încât persoanele să fie în control și să cunoască cum sunt evaluați și ce consecințe poate avea această evaluare, profilare sau decizie asupra lor.

Informațiile furnizate trebuie să fie suficient de cuprinzătoare pentru ca persoana vizată să înțeleagă motivele care au stat la baza deciziei sau profilării. În doctrină s-a arătat că informațiile pertinente privind logica utilizată ar trebui să cuprindă: a) informațiile despre datele personale prin intermediul cărora se ia decizia; (b) o listă a factorilor care influențează decizia; (c) o explicație rezonabilă despre motivul din spatele deciziei[1].

Varianta ideală ar fi ca persoana vizată să primească explicații cu privire la: a) informații detaliate despre datele personale utilizate; b) importanța fiecărei categorii de date în procesul decizional; c) calitatea datelor de învățare al algoritmului și tipul de modele utilizate; d) activitățile de profilare desfășurate și implicațiile acestora; e) valorile de eroare sau de precizie, în conformitate cu valorile corespunzătoare utilizate pentru a măsura eligibilitatea deducției; f) dacă există sau nu o intervenție umană în luarea deciziei; g) orice informații cu privire la audituri, în special cu privire la posibila deviație a rezultatelor deducțiilor, precum și certificarea sau certificările efectuate pe sistemele utilizate.

Valoarea internetului asupra societății moderne nu poate fi contestată, persoanele fizice și juridice bazându-se pe acesta pentru desfășurarea activităților și respectiv cu toții avem așteptări legitime privind disponibilitatea serviciilor internet, accesibilitatea și securitatea acestuia, inclusiv faptul că nu vor exista careva consecințe asupra drepturile și libertăților legitime.

Cu privire la riscurile sau consecințele utilizării identității digitale, acestea pot fi pe mai multe dimensiuni ale drepturilor omului, inclusiv:

1. Poate fi afectată libertatea de exprimare, prin faptul că persoanele care se simt supravegheate pot întâmpina dificultăți în a se exprima în mod liber în mediul online, de frica de a nu fi identificați, criticați.
2. Libertatea de informare poate fi lezată, prin faptul că furnizarea sau afișarea unui anumit conținut pe care algoritmii de profilare l-au considerat "relavant" pe baza unor căutări anterioare, ne poate de fapt priva de oportunitatea de a vedea alte informații noi, de exemplu, pe Facebook informația distribuită de prietenii noștri.
3. Ne poate influența luarea anumitor decizii, sau influența preferințele noastre prin afișarea constantă a unor informații/conținut similar.
4. Există riscul furtului de identitate, prin utilizarea în mod fraudulos a datelor care ne vizează din mediul online, sau prin spargerea, accesul ilegal la conturile noastre online.
5. Fraudarea prin metode de inginerie socială, care sunt în continuă amploare și diversificare. Ingineria socială, ca formă de manipulare utilizată de atacatori care urmărește de fapt obținerea datelor personale, date confidențiale, parole de acces, date bancare care sunt utilizate în mod fraudulos de către atacatori. Având o adresă de e-mail, un cont pe rețelele de socializare putem să recepționăm mesaje care ne îndeamnă la diferite acțiuni, inclusiv link-uri virusate, care odată accesate pot instala în dispozitivele noastre aplicații "rău intenționate" – malware care colectează despre noi informații personale. Datele obținute sunt utilizate de atacatori pentru a ne șantaja, pentru a ne sustrage banii de pe cardurile bancare.
6. Prelucrarea excesivă a datelor cu caracter personal și încălcarea dreptului de informare și acces la date, dreptului de opoziție asupra prelucrării datelor, dreptului la ștergerea datelor. Aceste drepturi sunt lezate atunci când operatorii nu informează corect persoanele vizate despre modul cum le prelucrează datele, ce date colectează, în ce scop le folosesc etc. Dreptul de opoziție este încălcat atunci când operatorii nu ne oferă posibilitatea să nu acceptăm prelucrarea unor date, de exemplu nu ne oferă posibilitatea

de a accepta sau respinge diferitele tipuri de cookies la accesarea paginilor web, prin faptul că acestea sunt bifate în mod implicit și nu putem să decidem respingerea acestora.

Cum ne protejăm de aceste riscuri?

- Prudența și informarea este întotdeauna modul ideal de a preveni aceste riscuri care le implică mediul online.
- Informarea înainte de a accepta anumiți Termeni și Condiții, înainte de a oferi datele ne poate ajuta să facem alegerea corectă de a oferi sau nu datele despre noi și a înțelege cum acetea vor fi prelucrate.
- Exercitarea dreptului de opoziție, prin respingerea notificărilor de marketing care nu sunt relevante, neacceptarea unor Termeni și Condiții care ar fi prea intruzive.
- Putem să ne exercităm dreptul la ștergerea datelor sau dreptul de a fi uitat. Google, cel mai mare motor de căutare are implementate formulare prin care putem să solicităm ca datele despre noi să fie șterse. Acest lucru a devenit posibil odată cu emiterea unei Decizii de către Curtea de Justiție a Uniunii Europene în 2014 – Google Spain[2], prin care Curtea a constatat că, odată cu trecerea timpului, diseminarea unor astfel de informații personale de către motoarele de căutare (care nu dețin propriu-zis informația, ci o afișează utilizatorului) poate contraveni dreptului la viață privată al cetățenilor UE. Curtea a concluzionat că obligația incumba motoarelor de căutare precum Google, Bing, Yahoo – de a nu mai afișa, după o anumită perioadă de timp, astfel de link-uri. Așadar, acești agenți au obligația ca, pentru căutările online în state aparținând UE, să nu mai redea utilizatorului link-uri către astfel de informații.
- Este recomandat să examinăm setările de confidențialitate pe rețelele de socializare prin care decidem cine ne poate vedea informațiile postate, inclusiv setarea preferințelor de publicitate pe social media.
- Respectarea regulilor de igienă cibernetică, de rând cu implementarea măsurilor tehnice de securitate – instalarea soluțiilor licențiate antivirus, utilizarea instrumentelor de tip VPN (rețea virtuală privată) care ne ascunde datele printr-o criptare online puternică, ascunzând activitatea de pe internet, evitarea utilizării rețelelor publice de Wi-Fi etc.

Toate măsurile enumerate supra, combinate împreună ne pot ajuta să reducem riscurile de a fi vulnerabili în fața amenințărilor care vin din mediul online.

Referințe bibliografice

1. Când decizia o ia maşina... Despre profilare, drepturi şi echilibru într-un univers digital. https://www.juridice.ro/698715/dreptul-omului-in-fata-masinii.html#_ftn108
2. HOTĂRÂREA CURȚII (Marea Cameră), 13 mai 2014. https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN
3. Legea privind protecţia datelor cu caracter personal, nr. 133 din 08.07.2011, publicată în Monitorul Oficial al Republicii Moldova, 170-175/492, 14.10.2011
4. Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), art. 22.
5. Uber will now deactivate riders with below average ratings. https://www.theverge.com/2019/5/29/18644143/uber-deactivate-rider-below-average-rating

Riscuri și soluții privind securitatea cibernetică în cazurile de alerte false cu bombe

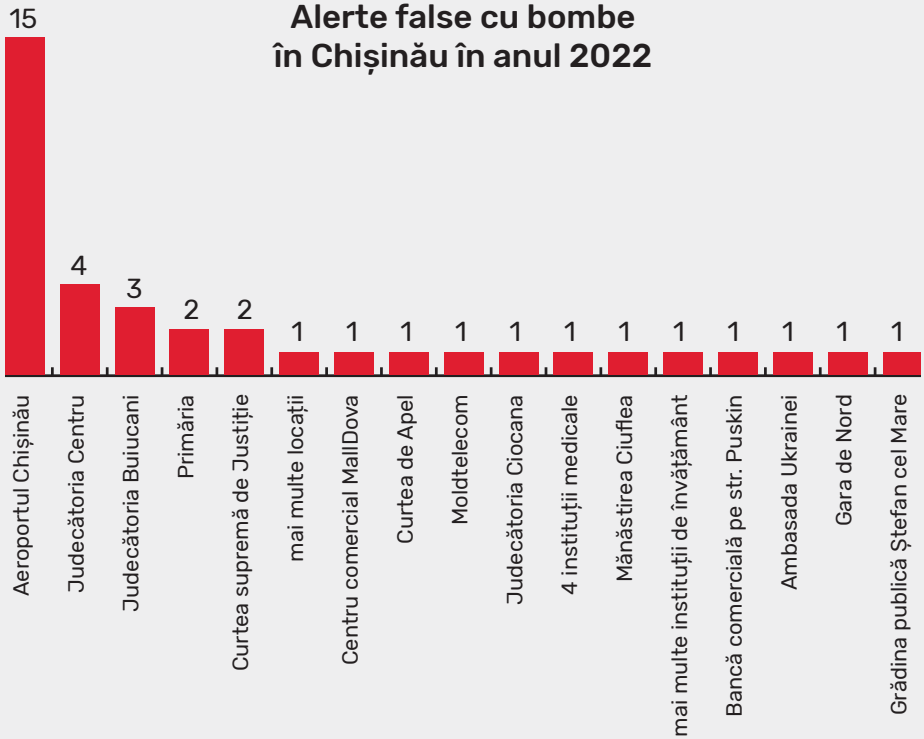
Gabriela DELEU

Specialist Calitate, Ingineria și Managementul Calității

Conform unei analize a evenimentelor care s-au întâmplat pe parcursul anului 2022 este vizibil un război hibrid, securitatea națională este continuu amenințată. Acțiuni subversive sunt cele 400 de alerte false cu bombe, iar aproximativ 380 fiind prin email, celelalte prin telefon. Graficul următor reprezintă un top al instituțiilor afectate de alertele cu bombe pe parcursul anului 2022 în Chișinău. Aceste atacuri afectează securitatea informațională și urmăresc anumite scopuri, fiind niște arme.

Pentru soluționare se cercetează cam 58 cazuri conform codului penal aceastea sunt comunicări mincinoase despre terorism. Conform informațiilor Serviciul de Informații și Securitate al al Republicii Moldova a fost identificat un minor de la sudul țării ce efectua aceste alerte activitatea căruia era dirijată din extern informațiile fiind înregistrate dintr-un stat European.

Însă alertele cu bombe nu se opresc nici în 2023, astfel pe 26 ianuarie și pe 9 februarie au fost 2 alerte cu bombe la sediul judecătoriei Buiucani. Efectuând o analiză de risc, se poate observa că în momentul alertelor false activitatea instituțiilor este oprită, iar momentul alertelor există o probabilitate mare ca rețelele de calculatoare nu sunt oprite (sunt funcționale). Astfel există riscul ca datele deținute în sistemul electronic să fie furate în acest interval de timp.Pentru a reduce acest risc este necesar de stabilit un plan de reacție în cazul alertelor cu bombe, astfel ca din exterior (în afara oricărui pericol) să existe o posibilitate de a deconecta rețeaua de calculatoare. O altă modalitate ar fi să existe un buton amplasat lângă ușa de ieșire care să fie apăsat, iar rețeaua de calculatoare să fie deconectată (un buton similar celui pentru incendii). Este important să fie stabilite un număr de persoane responsabile de securitatea datelor astfel în cazul de incident, să fie cunoscute responsabilitățile în securizarea datelor.



La moment sunt cunoscute instrumente și utilități pentru evaluarea nivelului de risc ce ține de securitate, sunt identificate mecanisme de îmbunătățire a automatizării schimbului de date privind securitatea cibernetică.

— **Baldrige Cybersecurity Excellence Builder (BCEB)** –este un instrument de evaluare pentru a ajuta organizațiile să fie eficace în eforturile privind securitatea și identificarea oportunităților de îmbunătățire în contextul întregii organizații.

— **Common Vulnerability Scoring System (CVSS)** – este un cadru deschis în comunicarea caracteristicilor și severității vulnerabilităților software-ului. Tabelul de mai jos exemplifică clasificarea severității:

CVSS v2.0 Clasificare		CVSS v3.0 Clasificare	
Severitate	Interval atribuit	Severitate	Interval atribuit
		Fără	0.0
Mică	0.0-3.9	Mică	0.1-3.9
Medie	4.0-6.9	Medie	4.0-6.9
Mare	7.0-10.0	Mare	7.0-8.9
		Critică	9.0-10.0

— **Security Content Automation Protocol (SCAP)** este un protocol automatizat ce deține conținutul de Securitate specificațiile și ideile comunității.

În contextul acestor situații nesigure, cum sunt alertele cu bombe, instituțiile afectate și alte instituții din Republica Moldova trebuie să:

— Creeze și să implementeze strategii privind securitatea cibernetică;

— Dețină forța de muncă implicată în securitatea cibernetică;

— Dețină o asigurare o rețea de aprovizionare de securitatea cibernetică eficientă și eficace;

— Protejeze sistemele și activele;

— Detecteze evenimentele cibernetice;

— Recupereze în cazul de evenimente cibernetice.

Referințe bibliografice

1. Alerta falsă cu bombă pe aeroportul internațional Chișinău. https://www.border.gov.md/index.php/ro/alerta-falsa-cu-bomba-pe-aeroportul-international-chisinau
2. Alerte cu bomba în țară în 2022 au fost deschise de aproape de trei ori mai multe față de 2021. https://echipa.md/2023/01/13/alerte-cu-bomba-in-tara-in-2022-au-fost-deschise-de-aproape-trei-ori-mai-multe-dosare-penale-fata-de-2021/
3. Articolele pe parcursul anului 2022 privind alertele cu bombeTV8.md
4. Autorul alertelor false cu bombe din sudul țării identificat. https://sis.md/ro/content/autorul-alertelor-false-cu-bomb%C4%83-din-sudul-%C8%9B%C4%83rii-identificat-de-c%C4%83tre-sis-%C8%99i-ini-al-igp

5. Directorul SIS despre alertele false cu bombe. https://www.zdg.md/stiri/stiri-sociale/directorul-sis-despre-alertele-false-cu-bomba-riscul-unor-destabilizari-este-mic-spre-mediu-dar-nu-este-exclus-niciun-scenariu/

6. Measurements for information security. https://csrc.nist.gov/projects/measurements-for-information-security/tools

Provocările la adresa spațiului cibernetic in contextul global actual

Luminița MIRON

Studentă Anul II, Masterat, Facultatea Relații Internaționale, Științe Politice și Jurnalism, Universitatea Liberă Internațională din Moldova

Transformarea digitală care se desfășoară în întreaga lume este, într-o mare măsură, o binecuvântare. Ea menține oamenii, întreprinderile și serviciile publice conectate. Cu toate acestea, progresul tehnologic major în domeniul tehnologiilor informației și comunicațiilor a dus la apariția unor noi forme de infracțiuni care nu pot fi urmărite și incluse în reglementările privind criminalitatea cibernetică, ceea ce indică faptul că fenomenul criminalității cibernetice, care vine odată cu dezvoltarea tehnologică, depășește cadrele sociale, etice, juridice, politice și de altă natură, existente într-o comunitate socială. Având în vedere că riscurile în materie de securitate cibernetică sunt globale, este logic să abordăm aceste amenințări printr-o abordare coordonată și colaborativă. Trebuie să ne asigurăm că există o strategie de abordare a riscurilor la adresa securității cibernetice, a protecției datelor, a vieții private și a siguranței online.

Definiția conceptuală a spațiului cibernetic

Conform NIST, spațiul cibernetic este un domeniu global din cadrul mediului informațional care constă în rețeaua interdependentă de infrastructuri ale sistemelor informatice, inclusiv internetul, rețelele de telecomunicații, sistemele computerizate, precum și procesoarele și dispozitivele de control încorporate.[1] Spațiul cibernetic le permite utilizatorilor să facă schimb de informații, să interacționeze, să schimbe idei, să se joace, să se angajeze în discuții sau forumuri sociale, să desfășoare afaceri și să creeze medii intuitive.

Spațiul cibernetic este o frontieră necunoscută care nu este încă controlată pe deplin. Atacurile cibernetice continuă să reprezinte o amenințare pentru rețelele de date din întreaga lume. Nici o sumă de bani, tehnologie sau hardware nu poate

1 NIST Glosssary https://csrc.nist.gov/glossary/term/cyberspace

asigura o protecție completă împotriva atacurilor cibernetice.[2] Mulți cred că o problemă poate fi rezolvată cu ajutorul tehnologiei, dar nu este întotdeauna așa. Veriga slabă în lanțul securității cibernetice fiind oamenii.

Numărul utilizatorilor de dispozitive mobile a crescut la nivel mondial, creând activități online inimaginabile și un nou ecosistem mobil. Astfel, pentru a satisface cererea în creștere, producătorii oferă publicului larg telefoane mobile, tablete și alte dispozitive ieftine, dar cu un nivel de securitate scăzut, ceea ce face și mai dificilă pentru autorități reglementarea cazurilor de încălcare a securității cibernetice. Fiecare țară are un set diferit de provocări în ceea ce privește combaterea criminalității informatice. Cu toate acestea, un lucru comun este acela de a avea un regim de securitate cibernetică substanțial, cuprinzător și implementabil pentru a opri eventualele pagube. Criminalitatea cibernetică a depășit demult granițele, ceea ce face dificilă pentru factorii de decizie politică formularea unor astfel de norme juridice care să aibă o acceptare universală.

Criminalitatea informatică este o infracțiune care se referă la orice tip de infracțiune care poate fi comisă cu, în sau împotriva sistemelor și rețelelor informatice. De fapt, criminalitatea cibernetică are loc într-un mediu electronic, ceea ce a dus la necesitatea de a crea așa-numita cultură cibernetică și securitate cibernetică. Atacurile cibernetice ne pot afecta în diverse moduri. Acestea afectează serviciile guvernamentale esențiale, cum ar fi sistemele financiare, asistența medicală, energia, aprovizionarea cu apă și multe altele. Securitatea națională și datele personale pot fi compromise și pot ajunge în mâini greșite. Mai rău, atacurile țintite pot duce la pierderea de vieți omenești.[3]

Spațiul cibernetic a evoluat încă de la începuturile sale, foarte rapid în întreaga lume. Războiul cibernetic, spionajul cibernetic și terorismul cibernetic sunt câteva dintre cele mai importante aspecte ale spațiului cibernetic care au făcut ca toate țările să fie îngrijorate în legătură cu păstrarea suveranității lor cu orice preț.

Spionajul cibernetic și războiul cibernetic

Sursele de amenințare s-au extins de la hackeri și până la teroriști, persoane din interiorul organizațiilor și națiuni străine implicate în spionaj cibernetic și război informațional. La fel și motivațiile s-au extins, începând cu câștiguri monetare până la avantaje politice, terorism cibernetic și putere strategică. O creștere

2 Is Cyberspace Secure From Humans? ISACA Journal vol 5 2021 https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2021/volume-5/is-cyberspace-secure-from-humans-joa-eng-0921.pdf

3 D. Vuletic, "Defending against threats in Cyber Space", Strategic Research Institute, Belgrade

rapidă a criminalității cibernetice și a activităților conexe a creat mai multe probleme pentru indivizi, agenții, sectorul privat și, mai important, pentru guvernul diferitelor țări. Criminalitatea cibernetică este un fenomen universal care atinge fiecare națiune în funcție de conectivitatea la internet sau de activitățile online ale acestora. Țările din lume se confruntă cu numeroase provocări tradiționale și netradiționale în materie de securitate precum și cu incapacitatea de a-și dota în permanență serviciile cu resurse moderne de informare și comunicare. Ca urmare, există o nevoie clară de cooperare între sectorul public și cel privat pentru a stabili politici democratice de control al securității cibernetice.

Războiul cibernetic reprezintă o serie de atacuri cibernetice împotriva unui stat-națiune, provocându-i un prejudiciu semnificativ. Acest prejudiciu poate include întreruperea sistemelor informatice vitale și chiar pierderea de vieți omenești. Războiul cibernetic este definit, în mod obișnuit, ca un set de acțiuni ale unei națiuni sau ale unei organizații de a ataca sistemele de rețele informatice ale unor țări sau instituții cu intenția de a perturba, deteriora sau distruge infrastructura prin intermediul unor viruși informatici sau al unor atacuri de tip "denial-of-service".[4]

Spionajul cibernetic a provocat mai multe daune și riscuri decât războiul fizic între națiuni. Cele mai valoroase informații privind securitatea națională stocate în computere sunt întotdeauna vulnerabile la atacurile cibernetice.[5] În zilele noastre, țările se acuză reciproc în mod constant de piraterie informatică pentru a obține secrete economice, militare sau politice în scopul de a câștiga putere strategică asupra țărilor vecine.

Dacă luăm ca exemplu războiul din 2022 dintre Ucraina și Federația Rusă, atunci Ucraina nu a fost primul "război cibernetic", dar a fost primul conflict major care a implicat operațiuni cibernetice pe scară largă. Invazia rusă, ineficientă până în prezent, în cadrul căreia operațiunile cibernetice au adus puține beneficii, ridică întrebări cu privire la echilibrul dintre apărare și ofensivă în spațiul cibernetic, dar și la utilitatea operațiunilor cibernetice ofensive și la cerințele de planificare și coordonare. Apărarea ucraineană mai bună decât se aștepta pare să fie o caracteristică a acestei invazii și principalul motiv pentru care eforturile cibernetice rusești au avut un efect limitat.[6] Deși este dificil să se ajungă la verdicte ferme cu privire la eficacitatea operațiunilor cibernetice legate de Ucraina (deoarece operațiunile cibernetice sunt adesea ținute secret), unele

4 What Is Cyberwarfare? https://www.fortinet.com/resources/cyberglossary/cyber-warfare
5 Cyberspace: An Emerging Security Issue in Global Politics https://www.theinternationalprism.com/cyberspace-an-emerging-security-issue-in-global-politics/
6 James A. Lewis, "Cyber War and Ukraine", Center for Strategic and International Studies (CSIS), Washington, D.C.

concluzii par destul de evidente. De exemplu, apărarea cibernetică a Ucrainei a fost remarcabil de rezistentă. Există mai multe surse ale acestei forțe defensive, în special priceperea, energia și determinarea organizațiilor cibernetice ucrainene, care s-au adaptat la campaniile ofensive rusești începând cel puțin din 2014.

Înainte de invazie, guvernele din întreaga lume se gândeau deja la strategii de securitate cibernetică pentru a contracara amenințările cibernetice din ce în ce mai mari din partea actorilor statali și a grupurilor criminale. Însă noile riscuri percepute de guverne începând cu luna februarie 2022 alimentează o nouă necesitate de a construi o reziliență cibernetică.[7] Nici o apărare nu este perfectă, dar eforturile Ucrainei au reușit până acum să contracareze atacurile cibernetice rusești. Această combinație de măsuri defensive este un pachet care poate fi duplicat de alte națiuni. O abordare bazată pe arme mixte, în cadrul căreia armele cibernetice sunt integrate cu alte mijloace ofensive, va obține toate avantajele.

Concluzii

Din cauza creșterii terorismului și criminalității cibernetice, este necesară organizarea sistematică a educației și întărirea centrelor operaționale militare, de informații, de poliție și civile pentru apărarea împotriva atacurilor cibernetice.

Războiul cibernetic și terorismul nu cunosc frontiere. Intervențiile în spațiul cibernetic trebuie să respingă ipotezele comune legate de timp și spațiu, deoarece astfel de atacuri, prin intermediul rețelelor moderne de informații și comunicații, pot fi efectuate de oriunde și într-un timp foarte scurt. Procesele de globalizare nu au avut un impact doar asupra realizărilor civilizației, ci și asupra dezvoltării unor noi amenințări la adresa civilizației. Cert este că terorismul și amenințările naționale s-au schimbat sub influența procesului de globalizare și a revoluției informaționale a Internetului. Avantajul strategic nu mai constă în puterea de luptă sau în localizarea geografică, ci în informație și cunoaștere. Cooperarea internațională și schimbul de informații sunt esențiale pentru prevenirea eficientă a amenințărilor cibernetice.

Noua dimensiune cibernetică a relațiilor internaționale reprezintă o provocare majoră pentru teoriile de conservare a puterii și de intimidare. Amenințările cibernetice sunt grave, destabilizatoare și în creștere. Atacul cibernetic, fie că se produce sub forma unui conflict între state, a unui act terorist sau criminal, acesta este un atac în spațiul cibernetic cu scopul de a compromite un sistem sau o rețea de calculatoare, dar și de a compromite sisteme fizice.

7 Cybersecurity: A global problem that requires a global answer https://www.welivesecurity.com/2022/05/27/cybersecurity-global-problem-requires-global-answer/

Referințe bibliografice:

1. Cybersecurity: A global problem that requires a global answer https://www.welivesecurity.com/2022/05/27/cybersecurity-global-problem-requires-global-answer/
2. Cyberspace: An Emerging Security Issue in Global Politics https://www.theinternationalprism.com/cyberspace-an-emerging-security-issue-in-global-politics/
3. D. Vuletic, "Defending against threats in Cyber Space", Strategic Research Institute, Belgrade
4. Is Cyberspace Secure From Humans? ISACA Journal vol 5 2021 https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2021/volume-5/is-cyberspace-secure-from-humans-joa-eng-0921.pdf
5. James A. Lewis, "Cyber War and Ukraine", Center for Strategic and International Studies (CSIS), Washington, D.C.
6. NIST Glossary https://csrc.nist.gov/glossary/term/cyberspace
7. What Is Cyberwarfare? https://www.fortinet.com/resources/cyberglossary/cyber-warfare

Importanța studierii securității cibernetice în școli

Irina CAZAN

Director adjunct pentru educație, IP Liceul Teoretic cu profil de arte „Nicolae Sulac”

Securitatea cibernetică este crucială în orice domeniu, dar nu în ultimul rând în educație. Atacurile cibernetice nu compromit, doar siguranța și securitatea profesorilor și a administrațiilor școlare, ci și confidențialitatea elevilor, în special, a minorilor din instituțiile de învățământ. Astăzi, milioane de elevi învață prin tehnologie în medii hibride, la distanță sau în clasă, navigând pe diverse platforme și site-uri,motiv pentru care siguranța este esențială pentru experiențele de învățare ale elevilor și munca profesorilor. Mulți dintre elevii noștri folosesc rețelele sociale ca o platformă pentru a a-și exprima sentimente, pentru a provoca discuții sau pentru a deveni cunoscuți. La fel de mulți dintre ei își doresc să fie primii care împărtășesc o știre, uneori ignorând dacă informațiile prezentate sunt adevărate sau nu.

Pentru adulți sunt inițiate diverse programe de studiere a securității cibernetice de către ong-uri, guvern, la nivel de corporații și platforme,însă utilizarea internetului nu se limitează la adulți, dar în această eră a tehnologiei și multimedia, cunoașterea securității cibernetice este, de asemenea, importantă pentru copii. Cu toate că internetul are un potențial imens și beneficii pentru elevi, utilizarea excesivă a internetului poate fi dăunătoare, având riscuri cibernetice, de exemplu, dependența de jocuri de noroc, pornografie, expunerea la informațiile personale și cyberbullying-ul. Un studiu recent al UNICEF arată că aproximativ 87% dintre elevii claselor a 6-12 sunt afectați de acest fenomen, fie că au fost victime, martori sau agresori.Criminalitatea cibernetică împotriva copiilor și adolescenților este cu siguranță o preocupare pentru părinți, mulți dintre ei își pun întrebarea: Ce face copilul meu în mediul online? Dar deseori nu ne dăm seama că el poate fi o victimă. Mulți părinți nu știu despre activitățile pe care le au copiii lor în spațiul cibernetic și că pot fi supuși la hărțuirea prin comentarii și insulte; intimidare, abuz sau exploatare sexuală.Deși despre siguranța online s-a discutat mai mult în ultimii trei ani, studiile naționale indică despre faptul că copiii utilizează Internetul mai mult. Cele mai problematice situații cu care se

confruntă copiii online vizează relaționarea și comunicarea online, în special cu persoane necunoscute, după cum urmează:

- 16,3% dintre copii au accesat involuntar imagini sau video cu caracter sexual;
- 8,1% dintre copii au fost încurajați să expedieze fotografii sau video cu părți intime ale corpului;
- 14,8% dintre copii au primit mesaje cu caracter sexual în mediul online;
- 10% dintre copiii, care au transmis poze persoanelor necunoscute, au primit propuneri indecente de la persoanele cunoscute pe Internet.

Multiplele riscuri la care se supun copiii în mediul online se află în strânsă legătură cu nivelul minim de implicare a părinților în educația despre siguranța cibernetică, abordarea sporadică și superficială în programul școlar.

În continuare, putem afirma cu justețe că rolul școlilor este important în predarea alfabetizării digitale, precum și în îndrumarea și informarea părinților cu privire la utilizarea internetului de către copii atât la școală, cât și acasă.

Obiectivul educației în domeniul securității cibernetice este de a educa utilizatorii tehnologiei asupra riscurilor potențiale cu care se confruntă atunci când folosesc instrumente de comunicare pe internet, cum ar fi rețelele sociale,chat, jocuri online, e-mail și mesagerie. Este primordial ca școlile să contribuie la cultivarea conștientizării securității cibernetice a elevilor mai detaliat, ci nu doar la orele de dezvoltare personală sau managementul clasei. Este esențial ca elevii moderni să fie educați cu privire la riscuri asociateși cumsă fie activi în spațiul cybernetic și care este importanța conștientizării securității cibernetice.

Viteza actuală de progres a tehnologiilor prezintă riscuri și provocări noi, astfel implementarea programelor de educație privind securitatea cibernetică vizează lipsa de competențe a profesorilor care reprezintă o provocare, mai ales atunci când se așteaptă ca aceștia să își instruiască elevii în domeniul securității cibernetice, prin urmare, instituțiile ar avea nevoie de profesioniști IT care pot găsi răspunsuri și soluții la provocări și pericole actuale, o altă soluție ar fi pregătirea profesorilor pentru a spori sensibilitatea față de progresul și schimbarea tehnologică și instruirea acestora prin programe de mentorat și conferințe de securitate cibernetică, astfel profesorii pot aborda temele legate de securitatea cibernetică la diverse discipline școlare. De exemplu, în cadrul orelor de română, engleză, franceză elevii po tprimi sarcini de scriere a unor eseuri privind conștientizarea securității cibernetice, ori în cadrul altor activități de învățare, cum ar fi dezbaterile concursurile, consiliile elevilor discursuri unde pot discuta diverse aspecte ale securității cibernetice, întroducerea de sisteme

de operare alternative celor obișnuite, acest lucru poate contribui la formarea elevilor în ceea ce privește conștientizarea securității cibernetice.

O metodă deja existentă și la fel de eficientă sunt activitățile desfășurate de către instituțiile de învățământ în cadrul Lunarului Securităţii Cibernetice care se desfășoară în luna octombrie și are ca scop: informarea și sensibilizarea privind riscurile online, a consolidării culturii digitale și sporirii nivelului de conștientizare privind amenințările din mediul online, precum și pentru modalitățile de protecție pe internet.

În altă ordine de idei, în 2019 a avut loc modernizarea curriculumului la disciplina Informatică pentru clasele VII-XII, fiind parte componentă a *Strategiei securităţii informaţionale a RM pentru anii 2019-2024* care la fel promovează securitatea cibernetică.

Aplicarea programelor de educație a securității cibernetice nu este suficientă,astfel școlile ar trebui să implementeze politici de conștientizare și educație în rândul minorilor cu privire la importanța securității cibernetice și măsuri de securitate care să garanteze protecția online a școlarilor. Prezența noilor tehnologii în clasă a devenit o provocare atât pentru părinții înșiși, cât și pentru profesori. Din acest motiv, educația în domeniul securității cibernetice este un factor cheie în garantarea siguranței online a copiilor. Formarea profesorilor în domeniul securității cibernetice pentru a acționa ca facilitatori ai informațiilor este esențială pentru a-i face pe elevi conștienți de importanța adoptării unui comportament online responsabil și sigur.

Referințe bibliografice

1. Pencheva, D., Joseph, H. and Awais, R. (2020) Bringing Cyber to School: Integrating Cybersecurity into Secondary School Education. IEEE Security & Privacy, 18, 68-74. https://doi.org/10.1109/MSEC.2020.2969409
2. Siguranța online a copiilor. Studiu de politici publice. https://lastrada.md/pic/uploaded/Raport_Siguranta_copiilor_online_2020_final.pdf

Integrarea și afirmarea securității cibernetice în aviație

Andreea POPA

Facultatea Relații Internaționale, Științe Politice și Jurnalism, ULIM

Lumea virtuală este punctul de cotitură care a schimbat tranziția unei alte ere – cea a digitalizării. Odată cu apariția și dezvoltarea noilor tendințe informaționale într-un timp record, zilnic, sunt create multiple actualizări și provocări. Sfera aviației, se numără și ea fiind "pradă" de consum ale acestora.

Securitatea cibernetică este unul din pilonii de bază care se preocupă în prim plan de încorporarea aspectelor dezvoltării și menținerii active siguranței și securității domeniului aeronautic. Este cea care promovează o cultură deschisă și competitivă odată cu măsurile și bunele practici spațiului cibernetic pentru creșterea calității unei integrări de succes în arena aviației naționale și internaționale.

Infrastructura aviației civile constă în sisteme interconectate cu componente de supraveghere, crescând astfel sensibilizarea la atacuri cibernetice.Chiar dacă aviația a înregistrat unele transformări benefice, înglobând sateliți, sisteme de transmitere a mesajelor la distanță cu ajutorul serverelor și echipamentelor receptoare, de emitere, bazându-se pe entitățile special responsabile de gestionarea vulnerabilităților cibernetice aflate atât la sol cât și în zbor, odată cu avansarea tehnologiei, continuă să se afle în pragul atacurilor cibernetice la nivelul managementului traficului aerian, serviciilor aeroportuare, mentenanței tehnice și restul lanțurilor de colaborare cu aceasta. Vectorii principali care intră în joc și produc mutații sunt diverse infracțiuni aduse la adresa securității, cum ar fi: jamming, hacking, spoofing.Un exemplu ar putea fi furnizarea semnalelor de tip (SIGKILL, SIGINT, SIGQUIT) care vizează perturbarea comunicării turnului de control cu aeronava aflată în curs de decolare sau aterizare. În acest caz, securizarea corectă a sistemelor informatice va oferi un punct de sprijin controlorilor de trafic aerian, cei care stau în spatele fiecărui zbor, asigurând siguranța spațiului aerian. Ilegalitățile date și fenomenele criminalității cibernetice sunt parte al terorismului cibernetic care au ca scop derularea informațiilor false de către anonimizarea,uneori prea reușită ai indivizilor din cadrul Echipelor Roșii.Toate acestea în conformitate cu eroarea factorului

uman țintesc asupra controlului aeronavelorpentru a avea ca scop provocarea catastrofelor sau atacarea anumitor puncte de interes. Numărul amenințărilor cibernetice continuă să crească exponențial în fiecare an, la fel ca și sofisticarea acestora. Importanța securității cibernetice este bine recunoscută, iar companiile aeriene și aeroporturile trebuie să investească în construirea unei baze solide de securitate.Având în vedere complexitatea și natura integrată a industriei transportului aerian, trebuie să ne mișcăm mult mai repede cu soluții bine construite în stabilirea unor apărări proactive pentru a ne asigura că rămânem în fața jocului utilizând pârghiile potrivite pentru a:

- Oferi o actualizare sistematică a software-ului și firmware-ului componentelor IT pentru remedierea vulnerabilităților de securitate ale oricărei infrastructuri critice;
- Aplicarea controalelor sistemelor existente din aviație pentru a detecta expunerea la atacuri și pentru a le asigura securitatea cibernetică fără a fi nevoie să le înlocuiască și să le refacă;
- Inovarea și proiectarea unei arhitecturi de partajare a datelor capabile să conecteze și să ofere acces la datele distribuite, păstrând în același timp confidențialitate;
- Efectuarea unei evaluări de securitate al elementelor care sprijină navigația aeriană, precum și a relațiilor dintre acestea, pentru a identifica și asigura o protecție adecvată împotriva escaladărilor în masă ale viitoarelor atacuri potențiale și a amenințărilor globale actuale.

La ora actuală, aviația Republicii Moldova, pe lângă înregistrarea din ultima perioadă a unui număr mare de alerte cu bombă false la Aeroportul Internațional Chișinău și odată cu schimbarea situației politice din țara vecină, poate fi ușor victima unor amenințări de securitate cibernetică.

Mai mult decât atât, Autoritatea Aeronautică Civilă și MOLDATSA trebuie să acorde o atenție sporită în continuare consolidării legilor în conformitate cu securitatea cibernetică pentru sprijinul unei structuri de mare capacitate care să reziste probei timpului. Aceasta ar trebui să implice navigația aeriană, comunicațiile, supravegherea, operațiunile și navigabilitatea aeronavelor și alte discipline relevante pentru a asigura siguranța și securitatea operațiunilor aviației civile.

Prin asumarea unui rol de lideri activi de susținerela astfel de provocărisunt OACI (Organizația Internațională a Aviației Civile), IATA (Asociația Internațională de Transport Aerian), EASA (Agenția Uniunii Europene pentru Siguranța Aviației Civile) care se află în poziții unice de a reduce sistematic riscul de securitate

cibernetică a aviației pentru membrii săi din întreaga lume, precum și de a asigura creșterea continuă a transportului aerian prin dezvoltarea unui cadru global de securitate cibernetică și crea în continuare parteneriate de lungă durată pentru intensificarea rezilienței aviației civile.

Drept urmare, folosind corect instrumentele de bază ale securității cibernetice, oferind însemnătate acestora, orice amenințare va fi ușor elucidată – Never TRUST, always VERIFY!

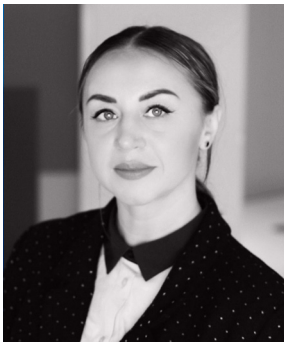
Referințe bibliografice

1. Centrul Național Cyberint, Glosar de termeni pentru domeniul securității cibernetice, 2019.
2. Stejarel Veres, Comunicarea între procese folosind semnale. http://labs.cs.upt.ro/labs/so/html/so7.html (accesat 12.03.2023)

Apărarea cibernetică: o prioritate tot mai mare pentru o dezvoltare durabilă

„Toți va trebui să schimbăm modul în care gândim despre protecția datelor."

Elizabeth Denham



Alina MUȘET

Ofițer superior, Secția juridică a Agenției Asigurare Resurse și Administrare Patrimoniu al Ministerului Apărării.

Membră a consiliului de administrare a Asociației Femeilor din Armata Națională.

Trăim într-o epocă de interconectare digitală tricotată cu premiere și inovații tehnologice. Trăim într-o perioadă cu schimbări rapide și oportunități transformatoare. Trăim într-o lume în care tehnologia a pătruns în aproape fiecare aspect al vieții noastre și nu mai este posibil să le separăm una de cealaltă.

Cu toate acestea, frumusețea și teroarea erei internetului plină de promisiuni și potențial remodelează radical lumea. Este ușor să vedem aceste provocări. Spațiul cibernetic este fără limite, deschis tuturor, conectând oamenii din întreaga lume, oferind orizont digital fără precedent pentru structura societății și dezvoltarea țării noastre. În același timp, societatea a devenit extrem de vulnerabilă în spațiul digitalizat, iar securitatea cibernetică a devenit o preocupare majoră, nu doar la nivel național, ci și global. Iar igiena și apărarea cibernetică devine o prioritate tot mai mare pentru a preveni agresiunile cibernetice și a tinde spre o dezvoltare durabilă.

Contrar credinței populației, obiectivul principal al securității cibernetice nu este acela de a proteja computerele, serverele sau rețelele. Cert este că, criminalitatea cibernetică vizează oameni și reputația întreprinderilor, iar tehnologia este mijlocul prin care au loc atacurile cibernetice.

Cu alte cuvinte, securitatea cibernetică se referă mai mult la protejarea indivizilor și povestește despre dezvoltarea proceselor de securitate și respectarea libertăților civile, mai puțin despre protejarea tehnologie. Altfel spus,apărarea cibernetică necesită adaptare, agilitate și cooperare între toți actorii care sunt interesați de păstrarea domeniului cibernetic ca spațiu de libertate securizat și durabil.

Actualmente, atât aplicativ, cât și practic putem observa un interes din ce în ce mai mare față de interconexiunea noțiunilor de securitate cibernetică și durabilitate. Acest interes nu este întâmplător. Tehnologiile digitale oferă atât oportunități extraordinare, cât și obstacole în realizarea obiectivelor de dezvoltare. Nu putem vorbi astăzi despre dezvoltare durabilă a oricărui sistem social fără a asigura securitatea lui în plan global, respectiv se evidențiază și corelația dintre tehnologie, apărare cibernetică și securitatea umană, fapt ce prezintă contribuția directă spre dezvoltarea capacităților de securitate cibernetică la realizarea Agendei 2030 pentru Dezvoltare Durabilă.

Din analiza celor 17 obiective pentru dezvoltare durabilă stabilite în agendă, se poate deduce că fiecare obiectiv include o componentă digitală. Poate fi găsită în mod explicit ca țintă în cadrul obiectivului 9 „Industrie, inovație și infrastructură", și este, de asemenea, menționată în țintele legate de schimbările climatice (obiectivul 13, 14 și 15), egalitatea de gen și abilitarea femeilor și fetelor (obiectivul 5), creștere economică (obiectivul 8), educație (obiectivul 4) și sănătate (obiectivul 3). Mai mult decât atât, impactul direct al evoluțiilor precum internetul, cloudul și inteligența artificială duce la o stare precară către progresul tuturor obiectivelor, în special, obiectivul 16 ,,Pace, justiție și instituții puternice".

Cu certitudine este faptul că, atacurile cibernetice vor accelera conflictele și vor eroda încrederea în instituțiile naționale și internaționale. Altfel spus, nesiguranța cibernetică afectează în același timp și potențialul de dezvoltare mai larg prin prisma parteneriatelor și atingerea obiectivului 17. Trebuie să recunoaștem că crearea păcii cibernetice și îndeplinirea obiectivelor pentru o dezvoltare durabilă sunt ambele provocări pe care nici o societate, instituție, organizație nu le poate îndeplini în mod solitar. Este necesară o cooperare, coordonare și parteneriate eficiente între părțile interesate pentru a construi bazele necesare unui spațiu cibernetic deschis, liber, sigur, rezistent și pașnic pentru toată lumea.

În rezultatul acestei analize, apare întrebarea...care este sarcina generală a securității cibernetice?S-au spus multe în presă despre ,,securitatea cibernetică", "amenințarea atacului cibernetic", iar politica tradițională de securitate cibernetică a fost abordată dintr-un punct de vedere național sau regional. Însă, la nivelul societății, au fost răspândite puține detalii despre amenințările cibernetice ce ar viza și afecta pe fiecare cetățean în parte. Nu este o claritate despre prevenirea acestor ilegalități cibernetice, pentru a oferi rezistența posibilă, precum și a repara daune cât mai repede posibil.

În acest sens, putem accentua abordarea națională despre domeniul de apărare cibernetică, consolidarea capacităților legislative, instituționale și ale societății civile pentru promovarea securității cibernetice și a conștientizării despre

igiena cibernetică. Care la rândul lor, ar oferi dezvoltarea unor noi mecanisme pentru schimbul eficient de informații, consultarea și coordonarea incidentelor cibernetice.

Importanța securității cibernetice este în creștere. Societatea noastră este mai dependentă din punct de vedere tehnologic decât oricând și nu există niciun semn că această tendință va încetini.

Adevărul este că, indiferent de vârstă, ocupație, profesie, suntem angajați la o întreprindere mică sau o instituție de stat, ne bazăm pe sisteme informaționale în fiecare zi. Tehnologia ne oferă o platformă atât la domiciliu cât și la muncă, și nimic nu ne împiedică să facem clic pe linkuri. Scurgerile de date care ar putea duce la furtul de identitate sunt acum postate public pe conturile de rețele sociale. Informațiile sensibile, detalii despre contul bancar sunt acum stocate în spațiul digital.Este vorba despre reputație și risc, despre provocări și amenințări, iar legătura dintre securitatea cibernetică individuală, instituțională, națională și globală este esențială pentru o stabiliate și pace durabilă.

În mod evident, există o nevoie urgentă de educarea cetățenilor pentru a fi mai pricepuți pe internet, formarea personalului prin programe și certificări legate de securitatea cibernetică.

La urma urmei, tehnologia este la fel de inteligentă ca și persoana care o folosește. Cunoașterea înseamnă putere, iar conștientizarea societății cu privire la amenințările cibernetice, securitateamobilă, igiena cibernetică,protejarea datelor și identității noastre, monitorizarea și raportarea cazurilor suspecte ar fi esențiale pentru peisajul securității cibernetice.

Realitatea este că ne confruntăm cu o curbă abruptă de învățare cu privire la amenințările în spațiul cibernetic. Iar pentru a stabili condiții pentru un sistem național funcțional, guvernul ar trebui să fie primul care dă dovadă de interes pentru o bună securitate cibernetică, prin stabilirea unei relații între sectorul public și privat, prin tratarea tehnologie ca pe o componentă de bază a dezvoltării infrastructurii și evoluția societății noastre.

Acest lucru este binevenit, mai ales având în vedere că orice intervenție în acest domeniu va avea nevoie de cooperarea dintre stat și companiile din sectorul privat. Deși cooperarea public-privată va fi esențială în crearea unui nou set de norme pentru timpul digital, ar trebui, de asemenea, să se bazeze pe o participare autentică și a cetățenilor.

Altfel spus, primul pas către apărarea împotriva oricăror potențiale amenințări digitale este în mâinile guvernului, instituțiilor, organizațiilor, precum și a fiecărui individ în parte. Pentru fiecare persoană din lume conectată la internet, este

esențial să se familiarizeze mai bine cu diferitele forme de atacuri cibernetice și cu instrumentele deja disponibile pentru a se apăra împotriva unor astfel de ilegalități.

Mai mult decât atât, este necesară crearea unei ,"rampe de salvare" pentru a ajuta persoanele să înțeleagă termenii tehnologici dificili asociați cu securitatea digitală, precum și o înțelegere mai generală a importanței securității în era digitală. Este vital ca fiecare să fie familiarizat despre securizarea conturilor de e-mail împotriva phishingului, utilizarea rețelelor și site-urilor web nesecurizate și a partajării parolelor. La nivel organizațional, despre securizarea hardware-ului cu o parolă complicată, criptarea și copierea de rezervă a datelor în mod regulat. Anume crearea unei culturi centrate pe securitatea cibernetică poate ajuta actorii societății să securizeze mai bine atât datele personale, cât și cele instituționale.

Trebuie să începem să înțelegem și să acceptăm că revoluția digitală va modifica structura societăților și vieților noastre, trebuie să ne întrebăm cum arată de fapt o societate liberă într-o lume digitală și ce forme iau drepturile noastre democratice online.

Iar progresul aici va fi un prim pas esențial pentru elaborarea bazei legale, pentru abordarea unui set de provocări în jurul libertăților digitale, pentru a crea rețele de supravegherea criminalilor cibernetici, care se prezumă a fi o cale dificilă la nivel global.Pe măsură ce amenințările cibernetice devin o nouă realitate, avem nevoie de un nou set de reguli.

Și doar cu politicile potrivite, cooperare, parteneriate,investițiile necesare în capacitatea umană, căutarea unor soluții centrate pe dezvoltare instituțională vom fi pregătiți pentru a cunoaște cum va evolua spațiul cibernetic,ce înseamnă asta pentru securitatea cibernetică,cum să protejăm segmentul uman, care este impactul asupra securității naționale,ce putem face pentru a ne asigura că securitatea devine mai bună. Sunt factori cruciali pentru lumea digitală în care trăim, iar cale spre o dezvoltare și pace durabilă va depinde doar de percepția indivizilor și implicarea guvernelor la nivel global.

Referințe bibliografice

1. Agenda 2030 pentru Dezvoltare Durabilă. https://cancelaria.gov.md/ro/apc/agenda-de-dezvoltare-durabila-2030
2. Cyber Security and Sustainable Development. https://ocsc.com.au/wp-content/uploads/2022/08/Cyber-Security-and-Sustainable-Development-2022.pdf (accesat 08.02.2023).
3. Cybersecurity in the environmental protection field. https://cybersecurityguide.org/industries/environmental-protection (accesat 07.02.2023);
4. Integrating Cyber Capacity into the Digital Development Agenda. https://thegfce.org/wp-content/uploads/2021/11/Integrating-Cybersecurity-into-Digital-Development_compressed.pdf (accesat 07.02.2023).
5. Revoluția în digitalizare continuă. 8 tendințe tehnologice pentru 2022. https://www.one-it.ro/blog/revolutia-in-digitalizare-continua-8-tendinte-tehnologice-pentru-2022/ (accesat 08.02.2023).
6. Secureworks. https://www.secureworks.com/blog/research-20913 (accesat 08.02.2023).
7. Sigur online. https://siguronline.md/ (accesat 09.02.2023).
8. Strategia securității informaționale a Republicii Moldova pentru anii 2019–2024 și a Planului de acțiuni pentru implementarea acesteia. https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro

Aspecte ale rezilienței cibernetice în statele membre ale NATO

Consolidarea securităţii cibernetice este "esenţială pentru creşterea rezilienţei societăţilor noastre şi pentru securitatea oamenilor noştri, pe timp de pace, în momente de criză şi în momente de conflict".

M. Geoană, Secretar General Adjunct NATO

Dr. Rodica Panța,

Lector universitar ULIM, Coordonatoare de proiecte IESPM

Spațiul cibernetic este o lume fragilă, instabilă și adeseori ostilă. Internetul a abolit frontierele geografice și temporale, cele dintre militari și civili, dintre spațiul public și privat. Este o provocare majoră să fii rezilient cibernetic în secolul XXI deoarece fiecare persoană poate deveni un actor activ sau pasiv în spațiul cibernetic, iar un echipament familiar ca smartfonul sau calculatorul se pot transforma în arme.

În contextul pandemiei Covid -19 o mare parte din activitatea economică, societală și educațională a fost mutată online, ceea ce a determinat necesitatea adaptării societății la inovațiile tehnologice și identificarea instrumentelor de creștere a rezilienței cibernetice sau preluarea celor elaborate în cadrul diverselor organizații.

Protejarea de amenințările cibernetice reprezintă o componentă cheie a apărării colective în cadrul NATO și are drept scop protejarea rețelele proprii (inclusiv operațiunile și misiunile) și creșterea rezilienței cibernetice în interiorul alianței.

Conceptele de securitate și reziliență cibernetică

Pentru a analiza conceptul de reziliență cibernetică trebuie să explicăm conceptul de securitate cibernetică. Termenii de securitate cibernetică și reziliență cibernetică sunt distincți, dar între ei există o legătură foarte strânsă. Securitatea cibernetică cuprinde tehnologiile, procesele și controlul efectuat pentru a proteja indivizii și organizațiile contra criminalității cibernetice. O securitate cibernetică

eficientă reduce riscurile atacurilor informaționale (Securitatea cibernetică este parte componentă a securității informaționale). Reziliența cibernetică are o abordare mai largă și este definită ca fiind modalitatea de a înțelege securitatea cibernetică într-un mod mult mai holistic având două axe principale:

a. o abordare preventivă și nu doar curativă;

b. creșterea rapidă a productivității în cazul unui atac computerizat[11].

Alfel spus, reziliența cibernetică se referă la apărarea contra atacurilor cibernetice potențiale și în același timp asigură supraviețuirea întreprinderii/ organizației în cazul unui atac[20].

Institutul Național de Standarde și Tehnologie (National Institute of Standards and Technology) a definit reziliența cibernetică ca fiind "capacitatea de a anticipa, rezista, recupera și adapta la condiții defavorabile de stres, atac sau compromitere a sistemelor care include resurse cibernetice" [9]. Această definiție are o sferă largă de aplicare, de la diverse entități la sisteme, infrastructuri, organizații sau națiuni.

Strategia de securitate cibernetică a României, din 2013, întocmită în conformitate cu standarde NATO, definește reziliența cibernetică (numită în document - reziliența infrastructurilor cibernetice) - capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic și de a reveni la starea de normalitate[19].

Definițiile analizate mai sus, ne permit să concluzionăm - reziliența cibernetică asigură atât securitatea cibernetică cât și continuitatea activității în cazul unui atac cibernetic.

Prevederi oficiale ale NATO privind reziliența cibernetică

Războiul din Kossovo (1999) a plasat problematica apărării cibernetice pe Agenda de securitate a NATO, dar la sfârșitul secolului XX, acest gen de atacuri au fost catalogate ca având un risc limitat ca amploare și potențial distructiv și care necesită doar răspunsuri tehnice[15].

Subiectul securității cibernetice nu a fost unul primordial pentru NATO, în perioada anilor 2001-2007. Era tratat doar din punct de vedere tehnic și nu a determinat un sentiment de urgență la nivel politic[10]. În timpul summit-ului de la Praga din 2002 problematică apărării cibernetice a fost menționată în Declarația Finală, deși în umbra altor probleme, cum ar fi lupta contra terorismului sau

proliferării balistice și nucleare. Un an mai târziu, în 2003, Alianța va semna un contract cu Finmeccanica, drept rezultat se va crea NATO Computer Incident Response Capability ce se focalizează pe detectarea și răspunsul la incidentele informatice. Având sediul la Mons, aceasta va trece la faza operațională în 2006 și va începe să funcționeze la capacitate maximă în 2013.

Anul 2007 reprezintă un an de cotitură în cadrul securității cibernetice a NATO. În acel an a fost înregistrat un atac asupra site-uri lor guvernamentale estoniene, ce le-a paralizat aproape total timp de trei săptămâni. Un an mai târziu, în 2008, site-ului președintelui Georgiei Mikhail Saakashvili, este piratat de hackeri care postează fotografii în care șeful statului este comparat cu Adolf Hitler. De asemenea, accesul Georgiei la site-urile BBC și CNN va fi blocat. Georgienii încearcă repede să răspundă atacului, dar, din nou, originea atacurilor este neclară: botnet[8]-urile responsabile sunt situate în Rusia, dar și în Canada, Turcia și ... Estonia[10].

Apărarea cibernetică a NATO devine un subiect tratat la cel mai înalt nivel în 2007, când este elaborată Politica NATO privind apărarea cibernetică, ce va intra în vigoare în ianuarie 2008. Câteva luni mai târziu, în timpul summitului de la București din aprilie 2008, au fost puse bazele a două organizații noi:

1. Autoritatea de gestionare a apărării cibernetice, responsabilă de coordonarea răspunsurilor aliate la potențialele atacuri cibernetice.
2. Centrul de Excelență Cyber Defense NATO, a fost înființat în Estonia la 16 mai 2008 pentru a efectua cercetări și a organiza conferințe pentru a explora dimensiunile strategice și juridice ale problemei.

Evenimentele din Estonia și Georgia influențează cu siguranță grupul de experți prezidat de Madeleine Albright în 2009-2010, care se ocupă de lucrările pregătitoare pentru noul concept strategic NATO în care apărarea cibernetică joacă un rol semnificativ. În noul concept adoptat la summitul de la Lisabona, i se dedică un paragraf întreg:

"... Forțele armate și serviciile de informații străine, criminalitatea organizată, grupurile teroriste și / sau extremiste sunt toate surse posibile de atac[10].

După summitul de la Lisabona, secretarul general NATO, Anders Fogh Rasmussen, a decis să creeze o nouă divizie în cadrul sediului central pentru a

8 Un botnet este o rețea care include o serie de dispozitive conectate la Internet, denumite boți. Termenul „botnet" este compus din cuvintele „robot" și „network" (rețea). Astfel, botneturile pot fi folosite pentru efectuarea de atacuri distribuite de tip denial-of-service (atacuri DDoS), furtul de date și trimiterea de mesaje spam, permițând atacatorului să acceseze dispozitivul și conexiunea acestuia.

face față "provocărilor emergente de securitate". Alături de teme strategice clasice, precum terorismul sau proliferarea armelor de distrugere în masă, există apărarea cibernetică. În plus, aliații au decis să revizuiască politica de apărare cibernetică formulată doar cu doi ani mai devreme. După un semestru de negocieri, noul document a fost aprobat în ședința miniștrilor apărării Alianței din 8 iunie 2012. Deși textul menționează despre necesitatea de a "oferi asistență aliaților pentru a obține un nivel minim de apărare cibernetică și pentru a reduce vulnerabilitățile infrastructurilor naționale critic documentul rămâne mai evaziv cu privire la amploarea acestei asistențe .

Oficial, start politicii în domeniul securității cibernetice s-a dat în timpul Summit-ului NATO din Țara Galilor (Marea Britanie) din septembrie 2014, în timpul căruia a fost adoptată Politica Întărită a NATO în domeniul apărării cibernetice ("Enhanced NATO Policy on Cyber Defence").

Ulterior problematica spațiului cibernetic s-a aflat pe agenda Summit-ul NATO de la Varșovia, în timpul căruia șefii de state și guverne s-au angajat politic să consolideze eforturile naționale în domeniul apărării cibernetice (îmbunătățirea rezilienței și a capacității de răspuns rapid și eficient la atacuri cibernetice, etc). În cadrul aceluiași Summit, a fost semnată Declarația comună de cooperare UE – NATO[14], privind consolidarea cooperării practice în anumite domenii. Organizațiile au căzut de acord privind sporirea participării în exerciții comune, stimularea cercetării, formării și schimbului de informații. Semnând aceste documente, statele membre și-au asumat obligația de a nu fi cibernetice ofensive, dar național-suverane în operațiuni NATO decât cu respectarea dreptului internațional, care este considerat cadrul principal pentru comportamentul statal în spațiul cibernetic, inclusiv pentru utilizarea capabilităților cibernetice ofensive[12].

În 2018, în timpul summit-ului NATO de la Bruxelles s-a instituit procesul permanent ce se referă la capabilități egale la nivelul fiecărui stat membru de a reacționa la atacuri cibernetice. Tot atunci, s-a luat decizia de a crea un Centru de Operațiuni pentru Securitate Cibernetică (CYOC – Cyber Operations Center). Scopul acestei organizații este de a furniza informații situaționale și coordonare a activităților operaționale ale NATO în spațiul cibernetic. În aceeași ordine de idei, în februarie 2019 a fost lansat Cyber Security Collaboration Hub, un hub informațional NATO unde aliații fac schimb de informații și de exemple în domeniul securității cibernetice.

Ghidul NATO a fost adoptat în anul 2019, în timpul reuniunii miniștrilor apărării ai NATO. Acesta stabilește un set de instrumente pentru dezvoltarea capacității alianței de a răspunde la activitățile cibernetice rău intenționate. În conformitate

cu acest document, Alianța trebuie să utilizeze toate instrumentele pe care le are la dispoziție, inclusiv instrumente politice, diplomatice și militare pentru a face față amenințărilor cibernetice. Ghidul include și opțiuni de răspuns care vor permite statelor membre să cunoască mai bine realitățile din spațiul cibernetic și acțiunile ce au loc în acest mediu, să își crească reziliența cibernetică, să conlucreze împreună cu partenerii în cadrul securității cibernetice.

Pandemia Covid /19 a avut o influență considerabilă și asupra securității și rezilienței cibernetice a NATO. La 3 iunie 2020, Alianța a publicat o declarație referitoare la atacurile cibernetice asociate perioadei pandemiei de Coronavirus. Acest document subliniază necesitatea unității blocului Nord-Atlantic în fața pandemiei și condamnă, în același timp atacurile cibernetice ce utilizează ca temă Covid-19 și sunt direcționate asupra instituțiilor cheie (spitale, servicii de sănătate și institute de cercetare,) care luptă contra virusului și se menționează că aceste atacuri pun în pericol viața cetățenilor.

Pe parcursul anilor Alianța a creat câteva organizații în domeniul asigurării securității și rezilienței cibernetice: Centru de Operațiuni pentru Securitate Cibernetică NATO CYOC (Cyber Operations Centre), Agenția NATO pentru Comunicații și Informații ("NATO Communications and Information Agency"/ NCIA), Centrul de Excelență NATO pentru apărare cibernetică de la Tallinn "NATO Cooperative Cyber Defence Centre of Excellence"/CCDCOE etc.

La 31 mai 2021 a fost deschis la București Centrului Euro-Atlantic pentru Reziliență. Inițiativa României privind înființarea și găzduirea Centrului Euro-Atlantic pentru Reziliență a survenit în contextul în care evaluările naționale, dar și ale NATO și UE relevă necesitatea intensificării eforturilor comune pentru gestionarea eficientă a unui spectru tot mai amplu de provocări. Acest centru își propune să contribuie la întărirea rezilienței NATO, UE și a statelor membre, precum și a statelor partenere.

Centrul își propune să devină o platformă pentru discuții strategice și dezvoltare de concepte, instruire și exerciții, precum și colectarea și furnizarea de lecții învățate și va permite dezvoltarea de diferite programe și inițiative în domeniul rezilienței pe următorii trei piloni:

1. Combaterea/reducerea riscurilor prin anticipare și adaptare;
2. Dezvoltarea de instrumente analitice și bune practici;
3. Cooperare practică în domeniul educației, instruirii și exerciții comune. Printre domeniile la care vor lucre diferite grupuri de experți se regăsește și reziliența cibernetică/ reziliența în domeniul tehnologiilor emergente și distructive[1]

Războiul din Ucraina și influența asupra securității cibernetice a NATO

Odată cu declanșarea războiului din Ucraina Departamentele de securitate cibernetică al NATO au urmărit îndeaproape războiul, atât pentru a găsi modalități de a ajuta Ucraina, cât și pentru a-și da seama cum să îngreuneze accesul Rusiei și al altor țări la infrastructură critică din statele membre NATO.

David Cattler Secretar General Adjunct în NATO pe partea de Informații și Securitate a menționat că în Ucraina au fost organizate o serie de atacuri cibernetice non-stop încă din februarie asupra serviciilor guvernamentale, asupra infrastructurii critice, asupra structurilor militare de comandă și control și, de asemenea, asupra internetului obișnuit și a comunicațiilor prin internet[14]. În scopul consolidării apărării cibernetice a Ucrainei, NATO începând cu anul 2014 a oferit diverse programe de formare și schimb de informații și de date. David van Weel, Secretar General Adjunct în NATO pe partea de Provocări emergente în materie de securitate menționează că acest lucru a contribuit la rezistența și capacitatea Ucrainei de a se apăra împotriva atacurilor Rusiei în spațiul cibernetic. NATO oferă în prezent acces Ucrainei la platforma NATO de partajare a informațiilor legate de cele mai noi programe malware (MISP), programe malițioase care pot spiona, altera, șterge sau bloca diferite tipuri de informații de pe sistemele pe care le infectează.

Războiul din Ucraina a confirmat odată în plus că spațiul cibernetic poate fi apărat și securizat doar în mod colaborativ, iar din acest punct de vedere alianța nord-atlantică derulează de mult timp programe și exerciții în comun cu toți aliații. Anul trecut, în noiembrie a fost organizat cel mai mare „poligon cibernetic" al Alianței - exercițiul Cyber Coalition 2022[5], care a avut încorporat și elemente învățate din experiențele recente cu Rusia. Exercițiul a reunit peste 1.000 de specialiști în securitate cibernetică din 26 de țări aliate, Finlanda și Suedia, Georgia, Irlanda, Japonia, Elveția, Uniunea Europeană, precum și din industrie și mediul academic. Pe parcursul a cinci zile, participanții au învățat să răspundă la

amenințări cibernetice, cum ar fi atacuri cibernetice asupra rețelelor electrice, programelor și activelor NATO și ale aliaților, îmbunătățindu-și astfel capacitatea de a apăra rețelele și de a colabora în spațiul cibernetic.

Războiul din Ucraina a adus în discuţie o nouă problemă: modul în care NATO ar răspunde la un atac cibernetic asupra unui stat membru - Cât de mare ar trebui să fie atacul cibernetic pentru a invoca activarea articolului 5 al NATO?

Concluzii

Atacurile cibernetice, noi și sofisticate din punct de vedere tehnologic, pot perturba sau chiar distruge funcții economice și societal vitale din cadrul NATO. Eforturile NATO pentru consolidarea rezilienței cibernetice s-au concretizat nu doar în documentele oficiale elaborate, dar și în diverse acțiuni pe care le desfășoară alianța cu statele nemembre, inclusiv cu Republica Moldova. Prin aceste activitățile NATO își intensifică eforturile de îmbunătățire a rezilienței cibernetice, continuând, în același timp să promoveze valorile euro-atlantice de libertate și democrație.

Referințe bibliografice

1. Centrul Euro-Atlantic pentru Reziliență - E-ARC. https://www.mae.ro/node/55849 (accesat 25.08.21)
2. Centrul de Cercetare și Instruire în domeniul Securității Cibernetice. https://fcim.utm.md/cercetari-stiintifice/centre-si-laboratoare-stiintifice/centrul-de-cercetare-si-instruire-in-domeniul-securitatii-cibernetice(accesat 21.08.21)
3. Cu sprijinul NATO a fost consolidată capacitatea Republica Moldova de răspuns la incidentele cibernetice. http://vectoreuropean.md/cu-sprijinul-nato-a-fost-consolidata-capacitatea-republica-moldova-de-raspuns-la-incidentele-cibernetice(accesat 28.08.21)

4. Cyberdéfense. https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=fr (accesat 26.08.21)

5. Exercise Cyber Coalition 2022. https://act.nato.int/articles/exercise-cyber-coalition-2022-concludes-estonia (accesat 15.02.23)

6. Fertasi Nadja EL, De Vivo Diana. Cyber resilience: protecting NATO's nervous system. https://www.nato.int/docu/review/articles/2016/08/12/cyber-resilience-protecting-natos-nervous-system/index.html (accesat 22.08.21)

7. Hotărâre cu privire la Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 nr. 811 din 29.10.2015 Monitorul Oficial nr.306-310/905 din 13.11.2015

8. În Moldova a intrat în vigoare Programul național de securitate cibernetică https://noi.md/md/news_id/72810 (accesat 28.08.21)

9. Introduction à la notion de cyber-résilience https://www.synetis.com/cyber-resilience-entre-mythe-et-pragmatisme/(accesat 23.08.21)

10. Joubert Vincent, Samaan Jean-Loup. L'intergouvernementalité dans le cyberespace : étude comparée des initiatives de l'Otan et de l'UE. În: Herodot 2014, nr.152-153 p. 261- 275.

11. Montérémal Jennifer. La cyber résilience, ou comment se protéger des attaques informatiques moderns. https://www.appvizer.fr/magazine/services-informatiques/protection-donnees/cyber-resilience (accesat 25.08.21)

12. Problematica securităţii cibernetice în cadrul organizaţiilor internaţionale şi implicarea României ca membru al acestora. https://www.mae.ro/node/28369(accesat 28.08.21)

13. Raport referitor la apărarea cibernetică. https://www.europarl.europa.eu/doceo/document/A-8-2018-0189_RO.html(accesat 24.08.21)

14. Războiul nevăzut purtat de Rusia și cu ce a surprins NATO: „E un domeniu care favorizează atacatorul" / Cum răspund Aliații și ce rol cheie joacă România. https://www.hotnews.ro/stiri-defense-25954690-razboi-rusia-nevazut-cibernetic-nato-cyber-coalition-romania-exercitiu-scenariu-amenintari.htm (accesat 12.02.23)

15. Revista NATO. Noi amenințări dimensiunea cibernetică (accesat 25.08.21)

16. Securitate cibernetică. https://mei.gov.md/ro/content/securitate-cibernetica(accesat 26.08.21)

17. Securitatea cibernetică pe timp de pandemie – subiectul principal al discuțiilor la „Moldova Cyber Week 2020"https://stisc.gov.md/ro/securitatea-cibernetica-pe-timp-de-pandemie-subiectul-principal-al-discutiilor-la-moldova-cyber (accesat 27.08.21)

18. Shea Jamie. La résilience, un élément clé de la défense collective. NATO review https://www.nato.int/docu/review/fr/articles/2016/03/30/la-resilience-un-element-cle-de-la-defense-collective/index.html?fbclid=IwAR0efAZI-ayoaKbveDyfjxR1f8bBWhZyOnDd08TGra40-ykjpOm4rvsdeHA (accesat 24.08.21)

19. Strategia de securitate cibernetică a Romaniei. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/StrategiaDeSecuritateCiberneticaARomaniei.pdf (accesat 24.08.21)

20. What is cyber resilience? https://www.itgovernance.co.uk/cyber-resilience (accesat 22.08.21).

Integrarea conceptului de securitate cibernetică în cadrul priorităților sistemului medical

Andreea GORAȘ

Studentă, Universitatea de Stat de Medicină și Farmacie "Nicolae Testemițanu"

În contextul circumstanțelor și situației în care se află Republica Moldova la momentul dat, componenta securității cibernetice trebuie să ocupe un loc primordial în cadrul strategiei securității naționale. Securitatea cibernetică include metode de protecție a sistemelor și rețelelor informatice, de atacurile cibernetice. Toate domeniile cu care interacționăm zi de zi, fie tangențial aspectului profesional sau personal, sunt interdependente de tehnologiile digitale pentru a avea o bună desfășurare a acestora. Anume tendința aceasta de modernizare și digitalizare a tuturor proceselor, care are drept scop ușurarea muncii noastre, oferirea un acces mai facil la toate serviciile utilizate, ne face totodată foarte vulnerabili în fața hackerilor. Putem afirma cu certitudine că această problemă este una foarte actuală și pentru sistemul medical.

Pentru sectorul medical, securitatea cibernetică trebuie să fie o prioritate, fiindcă odată cu cerințele medicilor de a avea la îndemână dispozitive medicale de ultimă generație, acces la baze naționale cu date ale pacienților, le scapă importanța creării unor condiții optime pentru securizarea acestora. Conceptul de securitate cibernetică este important cât pentru prestatorii de servicii medicale, atât și pentru companiile farmaceutice și de dispozitive medicale.

Industria sănătății a fost și va rămâne o țintă principală a atacurilor cibernetice. Începând cu 7 ianuarie 2022, Oficiul pentru Drepturi Civile al Departamentului de Sănătate și Servicii Umane al SUA (HHS) a investigat 860 de încălcări ale datelor raportate în ultimele 24 de luni; fiecare încălcare a expus informații de sănătate protejate (PHI) a 500 sau mai multe persoane. O sută nouăsprezece (sau 13,8%) dintre aceste încălcări au implicat „Asociați de afaceri" – furnizori și alte terțe părți care au avut acces la date sensibile ale pacienților – cea mai mare încălcare afectând 3,25 milioane de oameni. Conform Raportului privind costul unei

încălcări a datelor din 2021, realizat de IBM și Ponemon Institute, costul mediu al unei încălcări în domeniul sănătății a fost de 9,23 milioane USD, mai mult de două decât media de 4,24 milioane USD pentru toate industriile.

Foarte des ne confruntăm cu problema că întâietatea în clasamentul instituțiilor cu cel mai înalt grad de vulnerabilitate la atacuri cibernetice sunt spitalele. În pofida faptului că în cadrul instituțiilor medicale sunt implementate programe și sisteme integrate în structura informatică națională și sectorială, precum cel destinat utilizării de către medicii de familie, medicii specialiști și personalul medical, administrativ sau de conducere, care își desfășoară activitatea în cadrul unităților medicale din sectorul Asistența Medicală Primară, avem destul de numeroase lacune din cauza neprioritizării aspectului de securizare a datelor din aceste baze informaționale. Acest fapt se datorează lipsei cadrelor IT competente în instituțiile de stat, responsabile de componenta de securizare.

Dacă abordăm aspectul defecțiunilor echipamentelor medicale, putem afirma că uneori aceste incidente ne costă viața unui pacient. Aproximativ toate dispozitivele medicale conțin o componentă de software care ulterior se conectează cu alte dispozitive, pentru a obține o ulterioară monitorizare. Unele din cele mai cunoscute incidente, destul de uzuale, când pacienții cad drept victime ale atacurilor cibernetice sunt pentru cei ce utilizează pacemakerii (stimulator cardiac care furnizează miocardului impulsuri electrice regulate) și pacienții diabetici, cărora li se pot livra doze neadecvate, fie prea mari sau prea mici, prin intermediul pompelor de insulină. Mai drastică poate fi situația în care facem referință la aparate medicale utilizate la intervenții chirurgicale sau la monitorizarea post-operatorie a pacienților, confruntându-ne cu consecințe fatale - decesul pacientului.

Una din cauze ale creșterii atacurilor cibernetice în sistemul medical o reprezintă pandemia globală SARS-CoV-2. Anume datorită izolării pacienților la domiciliu și gradului sporit de utilizare a telemedicinii (transferul electronic la distanță al datelor medicale utilizând tehnologia telecomunicațiilor), vulnerabilitatea confidențialității datelor pacienților a ajuns la o cotă foarte înaltă. Telemedicina a generat un număr mare de potențiale escrocherii de tip phishing, deoarece pacienții trebuie adesea să acceseze un link dintr-un e-mail pentru a accesa serviciul repectiv. Astfel de tehnici pot fi, de asemenea, problematice pentru furnizorii de servicii medicale, deoarece hackerii încearcă aceste metode cu scopul de a pătrunde într-o rețea nesecurizată. O modalitate de combatere și prevenire a acestor atacuri ar fi adoptarea unui model ce presupune autentificarea cu mai mulți factori pentru orice încercare de conectare, precum și prin limitarea

accesului utilizatorului doar la informația indispensabilă acestuia, pentru ca un potențial hacker să poată accesa doar unele informații dar nu tot ce este stocat pe server.

Experții IT din domeniul sănătății consideră că este deosebit de dificil să mențină securitatea din cauza numărului enorm de echipamente medicale conectate, dintre care multe au specificații diferite și provin de la diferiți producători. Chiar dacă dispozitivele medicale nu includ neapărat o mulțime de date despre pacienți, ele pot servi drept puncte de acces ușor pentru hackeri la serverele care conțin o mulțime de date. Piața securității cibernetice în domeniul sănătății trebuie să acorde prioritate păstrării acestor puncte de intrare în siguranță și actualizate pentru a reduce costurile și daunele cauzate de accesul neautorizat.

Pacienții trebuie să cunoască metodele de comunicare sigure cu profesioniștii din domeniul sănătății. În plus, pacienții trebuie să fie conștienți de politicile de confidențialitate și securitate și să știe cum să își protejeze informațiile dacă interacționează virtual cu furnizorii lor de asistență medicală, medicii de familie, medicii de specialitate, fie prin intermediul unei platforme de telesănătate, vizite, mesagerie criptată sau altă metodă.

Medicii și colaboratorii instituțiilor medicale trebuie să cunoască regulile de confidențialitate și securitate ale organizației medicale. Instruirea regulată de conștientizare a securității pentru securitatea cibernetică a sănătății este crucială pentru a informa angajații despre riscuri și pentru a ști ce trebuie să facă în timpul incidentelor de securitate. În plus, angajații trebuie să știe la cine să apeleze pentru clarifica incidentele sau problemele. Înțelegerea a ceea ce funcționează și a ceea ce nu funcționează pentru a securiza infrastructura tehnologiei informației și datele, poate ajuta echipa de securitate cibernetică.

Drept concluzie putem specifica faptul că atacurile cibernetice în domeniul medical iau amploare și sunt în continuă creștere. Acest fapt nu trebuie să fie neglijat de Ministerul Sănătății, administrația instituțiilor medicale de stat și a clinicilor private. Componenta de securizare trebuie să constituie o prioritate, fiindcă de aceasta depinde confidențialitatea datelor cu caracter personal al pacienților; relația de încredere între medic/prestator și pacient și totodată de asta poate depinde însăși viața bolnavului.

Referințe bibliografice:

1. Cost of a data breach 2022. https://www.ibm.com/reports/data-breach
2. Cyber security in healthcare. https://www.knowledgehut.com/blog/security/cyber-security-in-healthcare
3. Data breach. https://www.cyberark.com/what-is/data-breach/
4. How we can secure the future of heathcare and telemedicine. https://dis-blog.thalesgroup.com/iot/2021/05/14/how-we-can-secure-the-future-of-healthcare-and-telemedicine

Dezinformarea prin intermediul rețelelor de socializare

Gabriela BOTEZATU

Facultatea Relații Internaționale, Științe Politice și Jurnalism, Universitatea Liberă Internațională din Moldova

În zilele noastre, informația devine una dintre resursele cheie care influențează funcționarea vieții economice, sociale și culturale a națiunilor moderne. Informațiile au, de asemenea, un impact din ce în ce mai mare asupra securității naționale a statelor. Dezvoltarea tehnologiei, internetului, universalitatea dispozitivelor de acces, rețelelor sociale, fac din informație un factor cheie care determină cunoașterea, puterea și, important, securitatea cetățenilor, a organizațiilor și a țărilor întregi.

Plus, perioada actuală este adesea descrisă ca fiind epoca știrilor false cu dezinformare, generate intenționat sau neintenționat, dar care se răspândește rapid. În prezent, există prea multe informații incomplete, informații înșelătoare și, cel mai important, prea multe informații (infodemie) care sunt înșelătoare și duc la haos informațional. Acest haos informațional are drept scop influențarea comportamentului uman, formarea opiniilor greșite dar și să ducă la destabilizare.

Majoritatea amenințărilor la adresa securității noastre sunt legate de securitatea informațiilor, ceea ce duce la o transformare semnificativă a sistemelor naționale de securitate. O astfel de amenințare este dezinformarea, care este folosită din ce în ce mai mult în mod intenționat.

Dezinformarea, miturile și știrile false proliferează în întreaga lume, cu consecințe potențial dăunătoare pentru siguranța publică, sănătate și comunicații eficiente. Dezinformarea este o astfel de modalitate de a furniza informații – adevărate sau false, pentru a induce în eroare în mod deliberat un grup selectat de destinatari și a-i convinge să se comporte în conformitate cu așteptările asumate. Dezinformarea este, prin urmare, o înșelăciune intenționată, cu cele mai grave consecințe pentru societăți în timpul situațiilor de criză.

Dezinformarea a fost folosită de mult timp pentru a eroda încrederea în autoritățile statului, pentru a crea tulburări sociale și pentru a obstrucționa obiectivele

statale și sociale legate, de exemplu, de problema securității, diverse conflicte, refugiaților sau a unei pandemii.

Dezinformarea, în contextul spionajului, informațiilor militare și al propagandei reprezintă difuzarea de informații voit false, cu scopul de a deruta inamicul cu privire la poziția proprie sau la intențiile de acțiune. Se referă și la distorsionarea unor informații reale, pentru a le face inutilizabile. După Vladimir Volkoff, autorul celebrului *Tratat de dezinformare*, dezinformarea este *tehnica ce permite furnizarea de informații generale eronate unor terți, determinându-i să comită acte colective sau să difuzeze judecăți dorite de dezinformatori*.

În timp ce propaganda are ca principal țel obținerea de sprijin emoțional, dezinformarea are scopul de a manipula audiența la nivel rațional, fie prin discreditatarea unor informații ce se contrazic, fie prin sprijinirea unor concluzii false. O a treia metodă de ascundere a faptelor este cenzura, aplicată atunci când un grup poate exercita un astfel de control. Atunci când canalele de informare nu pot fi închise complet, ele sunt făcute inutilizabile prin saturarea cu dezinformări, scăzând astfel valoarea "raportului semnal/zgomot". Dezinformarea nu trebuie confundată cu eroarea de informare, care nu este deliberată. De exemplu, dacă o persoană sau o agenție de știri difuzează o informație despre care nu știe că este adevărată, dar despre care crede că este adevărată, aceasta nu este o dezinformare propriu-zisă. De aceea, adesea dezinformarea este dată drept eroare de informare, atunci când acela care difuzează mesajul nu știe că acela care stă la originea mesajului a construit în mod deliberat o informație falsă, pe care a pus-o la dispoziție spre difuzare. Dacă scopul unei astfel de acțiuni este inducerea în eroare a utilizatorului final al informației sau dacă dezinformarea are rolul de a distruge credibilitatea celor suficient de creduli pentru a o difuza (de obicei, o agenție de știri), fără a-și da seama ce pagube îi produc receptorului final, trebuie judecat caz cu caz.

Într-un raport din 2017 al Consiliului Europei, care descrie dezinformarea ca fiind o „dezordine informațională", se menționează că acest concept de „știri false" se poate prezenta sub trei forme distincte:

1. **dezinformare neintenționată (misinformation)**. Informarea greșită este o informație incorectă sau înșelătoare. Diferă de dezinformarea, care este în mod deliberat înșelătoare. Zvonurile sunt informații care nu sunt atribuite unei anumite surse și, prin urmare, sunt nesigure și adesea neverificate, dar se pot dovedi fie adevărate, fie false. Chiar dacă este retrasă ulterior, dezinformarea poate continua să influențeze acțiunile și memoria. Oamenii pot fi mai predispuși să creadă dezinformare, deoarece sunt conectați emoțional cu ceea ce ascultă sau citesc.

2. **dezinformare deliberată bazată pe un fals (disinformation)** Dezinformarea se dovedește a fi informații false sau înșelătoare care au fost scrise și diseminate în mod deliberat în scopul manipulării. Scopul este, printre altele, de a provoca pagube economice, de a manipula opinia publică sau chiar de a genera profituri bănești. În zilele noastre, dezinformarea este produsă din ce în ce mai mult în formă scrisă și decorată cu imagini sau videoclipuri falsificate, în afara contextului și manipulate (așa-numitele falsuri profunde). Prin suportul tehnologic al, de exemplu, al boților sociali, al algoritmilor sau al inteligenței artificiale, dezinformarea este de obicei răspândită prin forumuri de pe Internet, site-uri de știri sau rețele sociale.
3. **dezinformare deliberată bazată pe un grăunte de adevăr (malinformation)** Informațiile defectuoase sunt informații care sunt adevărate și faptice, dar sunt transmise în mod intenționat pentru a provoca un prejudiciu real sau pentru a provoca amenințarea iminentă cu un prejudiciu asupra unei persoane, organizații sau țări.Exemple de informații defectuoase includ phishing, doxing, swatting și porno de răzbunare.Informațiile defectuoase ar trebui să se refere la informații adevărate și faptice care sunt transmise în mod intenționat de către difuzor într-un mod care provoacă un prejudiciu real sau amenințare iminentă de vătămare împotriva altei persoane. Nu ar trebui să fie folosit pentru a se referi la informații adevărate și faptice care pot fi utilizate (fie de către difuzor sau de către o terță parte) pentru a induce în eroare sau a jigni în alt mod o altă persoană.

Moldova se confruntă de mai mulți ani cu provocarea dezinformării externe și interne. Pericolele acestui fenomen sunt deosebit de evidente în campaniile electorale și în perioadele de criză națională, inclusiv pandemia de COVID-19, criza energetică, evenimentele geopolitice și războiul din Ucraina. Prezenta informare trece în revistă narațiunile de dezinformare predominante în Moldova din ultimii ani și măsurile corespunzătoare luate de autoritățile moldovenești pentru a combate acest fenomen. Acesta se încheie cu propuneri de îmbunătățire în continuare a cadrului legislativ privind dezinformarea și de creștere a capacității instituțiilor media din Moldova și a publicului de a recunoaște informațiile false.

Pe parcursul ultimilor trei ani, campaniile de dezinformare despre COVID-19 și vaccinare au circulat în Moldova pe diferite canale de comunicare, ajungând la un public țintă. Dezinformarea a ajuns în special la publicul din Moldova prin intermediul paginilor web religioase și al liderilor bisericești,al politicienilor actuali și foștilor politicieni, al comentariilor la articole, al postărilor pe rețelele de socializare și al profilurilor false de influenceri, printre alte surse. Un pas important făcut de autoritățile moldovenești în lupta împotriva dezinformării legate de COVID-19 a fost blocarea a numeroase surse de comunicare online care

răspândeau informații false și teorii ale conspirației despre această infecție. În conformitate cu Decizia Comisiei Naționale Extraordinare din 23 martie 2020, furnizorii de servicii de comunicații electronice accesibile publicului au fost obligați să blocheze paginile web care răspândesc informații false despre pandemie și vaccinare, pe baza unei liste de surse online publicate de Serviciul de Informații și Securitate al Republicii Moldova.

Cu toate acestea, nu toți furnizorii de internet s-au conformat, iar unele pagini web erau încă accesibile la câteva zile după ce a fost adoptată decizia de a le include pe lista neagră. Dezinformarea privind războiul din Ucraina Mass-media din Moldova se confruntă în prezent cu două probleme majore – dezinformarea internă și externă – care pot fi ambele legate de concentrarea proprietății media. Relația dintre concentrarea proprietății mass-media și dezinformare este relevantă deoarece publicul este manipulat și dezinformat în funcție de interesele celor care controlează mass-media. În aceste condiții, dezinformarea are puterea de a influența deciziile publicului său și poate schimba opinia unui cetățean cu privire la un anumit subiect.

Pentru a contracara acest fenomen, sunt necesare acțiuni bine planificate atât din partea autorităților statului moldovean, cât și din partea mass-media și a societății civile. Securitatea informațională este un element-cheie al securității statului și este imperativ ca autoritățile moldovenești să elaboreze o strategie de securitate informațională bine informată, care să servească interesele țării. Deși Parlamentul Republicii Moldova a adoptat o astfel de strategie în 2019, aceasta nu este adecvată pentru a contracara sau preveni dezinformarea Trebuie remarcat faptul că autoritățile moldovenești au luat măsuri pentru a îmbunătăți comunicarea dintre mass-media și instituțiile publice.

Chiar în prima zi a invaziei rusești în Ucraina, guvernul moldovean a anunțat crearea noului canal pe Telegram „Prima sursă", un canal oficial guvernamental de verificare a informațiilor, administrat de funcționari din cadrul Președinției, Parlamentului și Guvernului. Canalul include informații despre deciziile importante ale Guvernului Republicii Moldova și răspunde la zvonurile false din spațiul mediatic, inclusiv în ceea ce privește situația de securitate din Ucraina. Un alt pas important făcut de autoritățile moldovenești pentru a combate dezinformarea a fost adoptarea de către Parlament a așa-zisei Legi privind securitatea informațională, care a oferit instituțiilor statului instrumente de protecție a cetățenilor săi. Acest instrument legislativ a stabilit o interdicție privind emisiunile de știri și analitice din țările care nu au ratificat Convenția privind televiziunea transfrontalieră, inclusiv Rusia. Noua lege creează, de asemenea, o distincție pentru dezinformare, care implică sancțiuni mult mai aspre. În plus, a fost stabilit un nou prag de sancțiuni pentru cei care nu produc

conținut local. Important este că legea a înzestrat Consiliul Audiovizualului (CA) cu autoritatea de a suspenda dreptul de a face publicitate; în caz de dezinformare, CA poate suspenda licența unui mijloc de informare în masă pentru o perioadă de până la șapte zile. Aceste eforturi de restricționare a publicității reprezintă un instrument util în combaterea dezinformării.

Referințe bibliografice

1. UNESCO, Jurnalism, fake news și Dezinformare, 2021, https://unesdoc.unesco.org/ark:/48223/pf0000376919/PDF/376919rum.pdf.multi
2. Propaganda și Dezinformare pe timp de război https://mediacritica.md/podcast/propaganda-si-dezinformare-pe-timp-de-razboi/
3. Lilia Cravcenco-Zaharia, Contracararea dezinformării în Republica Moldova, Chișinău 2022 https://freedomhouse.org/sites/default/files/2022-11/fh-pb_18-Society-wide-Battle-Against-Disinformation_Rom-v3.pdf
4. What is disinformation? https://prevency.com/en/what-is-disinformation/
5. Pastila #9 De ce dezinformarea este o amenințare în adresa securității? Chișinău, 2022 https://infocenter.md/pastila-9-de-ce-dezinformarea-este-o-amenintare-in-adresa-securitatii/
6. Dezinformare și știri false (fake news) versus dispute interpretaționale în ceea ce privește istoria și conflictele memoriei. https://hi-storylessons.eu/wp-content/uploads/2021/05/1_L.Kaminski_Dezinformare-%C8%99i-%C8%99tiri-false-fake-news_RO-1.pdf

Securitatea la navigarea pe rețelele de socializare

Dina ROBU

Instituția Publică Liceul Teoretic cu Profil de Arte "Nicolae Sulac"

Securitatea modernă depinde foarte mult de comportamentul pe internet și rețelele sociale. Încrederea în rețeaua Internet este principalul pericol[1]. Încrederea în site-uri, furnizori de servicii și diferite sisteme de internet populare poate duce la o falsă senzație de siguranță. De exemplu, probabilitatea că Google să vă furnizeze un link care să conțină software rău intenționat este foarte mică. Însă întotdeauna pot exista metode cu ajutorul cărora hackerii pot depăși sistemele și elementele de securitate, chiar și pe cele ale organizațiilor cu renume. De fapt, majoritatea atacurilor cibernetice de succes se bazează pe faptul că victima se simte în siguranță în mediul său, fie pe un site web, fie într-un birou [2]. Rețelele sociale sunt adesea folosite pentru atacuri cibernetice țintite, aceasta se numește inginerie socială. Cum să nu deveniți o victimă a ingineriei sociale:

- Opțiunea cea mai puțin riscantă ar fi să nu acceptați niciodată o cerere de "prietenie" pe o rețea socială de la o persoană pe care nu o cunoașteți sau a cărei identitate nu o puteți confirma.
- În timpul unor atacuri de inginerie socială, conexiunile personale pe rețelele sociale sunt folosite pentru a aduna informații suplimentare despre persoana în cauză. Așadar, chiar dacă primiți o cerere de la o persoană cunoscută, în spatele acestui profil poate exista un hacker. Întotdeauna utilizați un canal de comunicare alternativ pentru a vă asigura că persoana cu care comunicați pe rețelele sociale este de fapt acea persoană. Deoarece conturile de pa rețelele sociale pot fi ușor falsificate, sparte sau discreditate pentru atacuri țintite.
- Există diferite tipuri de rețele sociale. Fiți deosebit de atenți în "rețelele profesionale", unde abonații fac în mod regulat schimb de CV-uri, recomandări și cereri de angajare. Acolo oamenii sunt mai interesați să-și dezvolte rețeaua, iar interacțiunea cu străinii este mai frecventă, chiar încurajatoare. În același timp, nivelul de atenție al utilizatorilor tinde să scadă.

Cea mai simplă regulă pe care trebuie să o reținem pentru a ne proteja pe o rețea socială este să nu facem click pe mesaje și link-uri despre care nu sunteți siguri sau nu știți ce ar putea fi în spatele lor. O metodă bine-cunoscută de distribuire a programelor dăunătoare este o aplicație care promite utilizatorilor Facebook să le arate persoanele care le-au vizitat profilurile. Alte tipuri suspecte de "aplicații" promit să vă spună cine ați fost într-o viață anterioară, ce origini aveți și ce înseamnă de fapt numele D-voastră. A face click pe astfel de link-uri poate fi periculos[3,4]. Astfel, nu utilizați jocuri, programe și alte activități pe rețelele sociale care implică furnizarea de informații personale. Este important să țineți minte că aproape fiecare site web de pa internet poate conține software rău intenționat. Așadar, toate site-urile web pe care le utilizați pot reprezenta un potențial pericol. Hackerii aleg de obicei site-uri în care, după părerea lor, utilizatorii au încredere. Așadar, ei folosesc un fals sentiment de securitate și încredere al utilizatorului. Tuturor ne place să ne distrăm online însă trebuie să acordăm o atenție sporită pe rețelele de socializare, deoarece distracțiile sunt cel mai des expuse riscului de infectare cu software rău intenționat sau furt de identitate.

Reguli de siguranță pe site-uri web:

- Nu răsfoiți pagini web dacă ați intrat pe un dispozitiv cu drepturi de administrator. Creați conturi separate pentru administrarea dispozitivului și utilizarea lui în mod regulat. Utilizați drepturile de administrator doar dacă este necesar, de exemplu, pentru instalarea programelor. Pentru utilizarea de zi cu zi , utilizați setările obișnuite de utilizator.
- Utilizați conturi separate pentru copii sau alte persoane atunci când utilizați un computer comun și instalați control parental pentru copii.
- Asigurați-vă că software-ul utilizat pe computer este actualizat în mod constant. Utilizați cel mai recent browser web și actualizați-l în mod constant.
- Instalați un browser pentru navigare sigură. Utilizați programe browser care blochează anunțuri, ferestrele de tip pop-up și videoclipurile cu redare automată pentru a vă proteja confidențialitatea.
- Nu utilizați funcția "Reține parola" în browser-ele web.
- Asigurați-vă că site-urile web sunt autentice, mai ales când introduceți informații private sau confidențiale. Dacă site-ul web oferă o conexiune *https*, alegeți să o utilizați după ce vă asigurați că certificatul de securitate este valabil.
- Când postați informații personale pe platformele rețelelor sociale, gândiți-vă la confidențialitate și securitate cibernetică.

Astăzi aproape toate serviciile folosesc autentificarea prin parolă [5]. Parolele trebuie să fie cât mai complexe, să conțină litere mici și mari, caractere speciale (chiar spații) și cifre. Totodată, ele trebuie să conțină cel puțin 12 caractere. De obicei acest lucru înseamnă că parolele sunt foarte greu de reținut. O soluție posibilă [6] ar fi să combinați o parolă din diferite cuvinte sau expresii pentru a fi mai ușor de reținut. De exemplul:

- BXin79cat4^ng!"
- 12345678
- bgonxi
- O,v,cp,@,pfn; Sv2 o!mf.V!H!@v;U2 Lt;

Observăm că prima parolă BXin79cat4^ng!"este puternică și îndeplinește multe standarte de siguranță. Dar, totodată există un dezavantaj foarte mare – este greu de reținut și aceasta poate tenta utilizatorul să noteze parola și să o păstreze undeva pe o foaie de hârtie. Următoarele parole 12345678 și bgonxi sunt exemple ale celor mai comune și simple parole care pot fi sparte. O parolă care utilizează o combinație de nume și număr de telefon unei persoane este, de asemenea, relativ ușor de spart. Cea mai bună opțiune este ultima parolăO,v,cp,@,pfn; Sv2 o!mf. V! H! @v; U2 Lt;,ea este de încredere datorită lungimii sale. Parola conține litere mici și mari, caractere speciale (spații) și cifre. De asemenea este ușor de reținut, deoarece sunt versuri de a lui George Bacovia:

O, vino, cel puțin, acum, prin forțele necunoscute;

– Să viu?
– Oh! mi-i frică.
– Vezi!
– Hai!
– Am venit;
– Unde?
– Lângă tine;

Este foarte important să utilizați parole diferite pentru sisteme diferite și să le schimbați în mod regulat. Totodată, parolele trebuie păstrate în secret. Există programe speciale dezvoltate pentru a crea și stoca parole puternice unice, care sunt cele mai sigure de utilizat. Se numesc "manager de parole". Trebuie să țineți minte doar o singură parolă lungă, unică și sigură, care vă va ține blocat managerul de parole. Dacă utilizați deja un manager de parole pentru a crea parole sigure, atunci, recomandăm în timpul înregistrării, să adăugați un caracter suplimentar la fiecare parolă pentru o siguranță mai mare. Vă putem recomanda: LastPass https://www.lastpass.com/, KeePass https://keepass.info/ , Dashlanehttps://www.dashlane.com/

Referințe bibliografice

1. Ghid practic pentru OSE. Implementarea măsurilor minime de asigurare a securității rețelelor și sistemelor informatice. Editura Sitech 2021. https://dnsc.ro/vezi/document/ghid-ose (accesat 05.02.2023)
2. Alexandru Angheluș. Tentativă de infectare cu malware – Campania "Documentul de la bancă". 2023. https://www.prodefence.ro/tentativa-de-infectare-cu-malware-campania-documentul-de-la-banca/ (accesat 07.02.2023)
3. Alexandru Angheluș. Divulgarea de informații prin imprudență. https://www.prodefence.ro/divulgarea-de-informatii-prin-imprudenta-transmitere-colectare-exploatare/ (accesat 08.02.2023)
4. Alexandru Ciprian Angheluș, Oana Buzianu, Mircea Constantin Șcheau. Cyber Intelligence – Using Profiling. ISACA 2023.https://www.researchgate.net/publication/352742564_Cyber_Intelligence_-Using_Profiling (accesat 11.02.2023)
5. Alexandru Angheluș. Cybersecurity course. CyberHygiene. "Women in Security and Peacekeeping: Building diversity, accessibility, and strongerteams"https://womenincyber.md/ (accesat 04.02.2023)
6. Global Cybersecurity Outlook 2023. Insight report january 2023. World Economic Forum. https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf (accesat 06.02.2023)

Interviuri

Ivana Arapu

12 ani de experienţă în domeniul comunicaţiilor electronice şi tehnologiei informaţiei. În prezent activează în cadrul companiei Orange Moldova în calitate de Head of Corporate Security şi Data Protection Officer.

Pentru a încuraja o dezvoltare durabilă a unei companii şi o abordare corporativă responsabilă socială, consideră că domeniul de securitate trebuie să fie privit într-o manieră globală. Întrucât ameninţările se află în continuă schimbare, iar complexitatea şi diversitatea acestora sunt în creştere, este de necontestat faptul că nu mai putem trata aspectele individuale ale securităţii în mod izolat: sănătatea şi securitatea ocupaţională, securitatea fizică a activelor, securitatea mediului, securitatea reţelei şi a sistemului IT, securitatea datelor cu caracter personal, etc..

Ea consideră că mai mult decât oricând este necesară sporirea gradului de conştientizare în domeniul securităţii şi dezvoltarea culturii sociale în spaţiul informaţional.

1. Ce v-a atras iniţial către domeniul securităţii cibernetice şi cum v-aţi dezvoltat cariera în acest domeniu?

Deseori mi se pune această întrebare, dar răspunsul este unul simplu, m-a atras aspectul de curiozitate şi incertitudine.

Activez în domeniul de telecom aproape de 12 ani. Am ocupat diferite funcţii atât la nivel ierarhic cât şi alte domenii de activitate, precum: vânzări, geomarketing, business intelligence, deservire clienţi, prevenire fraude şi asigurare venituri, etc.. Am gestionat echipe de peste 60 de angajaţi. Efectiv, am avut oportunitatea de a gusta câte un pic din diferite ramuri ale sectorului telecom. Vreo 4 ani în urmă am trecut printr-un burn out, unde simţeam că am nevoie urgent de o schimbare. Eram în căutarea unui domeniu de activitate mai dinamic, care să mă reprezinte şi să mă ţină mereu conectată. Problema majoră pe care o întâmpinam era incertitudinea privind direcţia de urmat, şi domeniul în care să-mi redirecţionez cariera, deoarece nu mă regăseam nicăieri (mă simţeam dezorientată/ resimţeam un sentiment profund de neîmplinire). Aveam momente când contemplam ideea de a renunţa la tot şi de a căuta noi orizonturi în străinătate, pornind de la zero.

Într-o bună zi, am văzut anunțul de angajare pentru poziția de Șef Securitate Corporativă, Orange Moldova. Nu se cerea obligatoriu să ai studii în IT, se căuta o persoană cu o gândire sistemică, bazată pe risc. Îmi doream extrem de mult această poziție, fiind impresionată în primul rând de perimetrul responsabilităților și de faptul că securitatea cibernetică presupune unul dintre cele mai populare/solicitate domenii în prezent, cu amenințări și provocări noi care apar în fiecare zi, ceea ce cu siguranță îmi satisfăcea dorința de a găsi o activitate dinamică în continuă evoluție. Respectiv în Martie 2020 mi-am început cariera într-un domeniu cu totul diferit pentru mine.

2. Care a fost cea mai mare provocare pe care ați întâmpinat-o ca femeie în domeniul securității și cum ați depășit-o?

Provocările cu care m-am confruntat, și continuu, cu siguranță nu țin de faptul că sunt „femeie".

Mi-am început cariera în securitate concomitent cu criza Pandemică care a debutat în martie 2020. Aveam în responsabilitate asigurarea continuității afacerii într-un context în care peste 1000 de angajați au trebuit să activeze la distanță, efectiv regândindu-le nivelele de acces la sistemele informaționale ale companiei și în același timp asigurând un nivel adecvat de protecție împotriva infectării acestora cu virusul Covid-19.

Ulterior a urmat războiul din regiune și nemijlocit criza energetică.

Mă consider norocoasă să-mi desfășor activitatea într-o corporație unde valorile angajaților, clienților sunt considerate în prim plan. Astfel, când ai tot suportul și înțelegerea managementului cu siguranță reușești să depășești orice provocare.

3. Care sunt câteva dintre realizările de care sunteți cea mai mândră în cariera dvs. în securitatea cibernetică?

Nu voi menționa despre sisteme de securitate, fie controale de securitate aplicate întru asigurarea protecției împotriva atacurilor cibernetice.

Sunt mândră în primul rând că am reușit să creez o echipă de specialiști, fiecare în subdomeniul său. Există, într-adevăr, un imens deficit global de talente în domeniul securității cibernetice, iar abordarea cu succes a acestei provocări se dovedește a fi extrem de dificilă. Un alt aspect constă în creșterea semnificativă a nivelului de conștientizare privind importanța securității informaționale în rândul angajaților. Cel mai exploatat vector de atac cibernetic, cel puțin în acest

deceniu, sunt oamenii. Astfel, dacă o companie reușește să implementeze un „People Firewall" atunci cu siguranță face față oricărui tip de atac cibernetic.

Avem un obiectiv cheie ca societate, pe care trebuie să-l realizăm, şi anume implementarea unei culturi de securitate, dezvoltată prin educație.

4. Ce sfaturi aveți pentru femeile interesate de a-și urma o carieră în securitatea cibernetică și cum să-și depășească eventualele obstacole?

În primul rând au nevoie de încredere în propriile forțe, atitudine corectă, dedicație şi integritate.

Am menționat inițial „soft skills", deoarece consider că aceste abilități stau la baza oricărui job.

Dacă o persoană vrea să îmbrățișeze o carieră în cybersec, atunci trebuie să fie pregătit să învețe în mod continuu, să rămână mereu informat cu evoluțiile din mediul cibernetic şi cu apariția de noi instrumente destinate pentru a răspunde incidentelor de securitate. Nu este un job care se rezumă la un proces de învățare într-o perioadă determinată urmat de livrarea unor sarcini. Din păcate inginerii de securitate sunt cu un pas în urma atacatorilor, motiv pentru care „continuous improvement is the success key in cybersec".

Astfel, trebuie să fii pregătit(ă) să faci față faptului că, alegând o carieră în securitatea informațională, nu vei putea avea un program de lucru fix, pentru că în orice moment urmează să fii pregătită pentru a răspunde unui incident de securitate, crize. Astfel, dacă la nivel de mindset îți e dificil să accepți acest lucru, atunci cybersec poate să nu fie potrivit pentru tine.

5. Cum puteți încuraja și inspira alte femei să se implice în domeniul securității cibernetice?

Vreau doar să menționez că astăzi securitatea cibernetică nu trebuie relaționată nemijlocit sferei IT.

În acest deceniu, dezinformarea, problemele din lanțul de aprovizionare, erorile umane sunt în topul riscurilor din domeniul securității cibernetice. Astfel, un job în cybersec nu este rezervat exclusiv bărbaților, deoarece în realitate există foarte multe activități unde o femeie ar face față mai bine sarcinilor.

Curajul şi dedicația sunt esențiale pentru pentru femeile care doresc să înceapă o carieră în cybersec.

6. Cum vedeți evoluția rolului femeilor în securitatea cibernetică în viitor și care sunt provocările și oportunitățile pe care le observați?

Conform datelor statistice, femeile reprezintă 25% din totalul forței de muncă în industria de securitate informațională. După mine, femeile din domeniul securității cibernetice se confruntă cu o realitate de necontestat: deseori ele sunt singura femeie dintr-o încăpere în care predomină bărbați – ceea ce poate fi unul dintre motivele pentru care decid să nu urmeze o carieră în acest domeniu. Este important de subliniat că absența femeilor din industria de cybersec poate crea un cerc vicios: cu cât mai puține femei activează în securitatea IT, cu atât mai multe tinere care ar putea fi atraşi de acest domeniu, s-ar putea să-și piardă interesul în el.

Atunci când sunt întrebate femeile de ce nu au ales o carieră în domeniul securității cibernetice, majoritatea răspund că: nu au experiență în codare, nu sunt interesate de computere, nu cunosc de existența securității cibernetice și că nu sunt suficient de bune la matematică. În mod clar, problema este una de conștientizare, deoarece astăzi companiile nu mai caută doar specialiști care să scrie cod. Calități precum gândirea critică și rezolvarea de probleme sunt la fel de importante în securitatea cibernetică, însă, din păcate, industria este percepută în exterior predominant ca fiind axată pe aspectele tehnice.

7. Care sunt cele mai valoroase abilități și competențe pe care le considerați necesare pentru succesul în domeniul securității cibernetice?

Atitudinea, şi implementarea conceptului de „zero trust" la nivel de mindset.

8. Ce vă motivează să continuați să lucrați în securitatea cibernetică şi care este viziunea dvs. pentru viitorul femeilor din acest domeniu?

Dacă te-ai atins vreodată de cybersecurity, vei rămâne acolo pentru totdeauna.

Dacă ne dorim mai multe femei în domeniul de securitate sau IT atunci trebuie să dăm la o parte stereotipurile. Eu cred că femeile ezită mai mult să urmeze cariere în domeniul tehnologiei, deoarece sunt învățate să aspire la perfecțiune, în timp ce bărbații sunt încurajați să-și asume riscuri – spre deosebire de teoria lui Damore despre diferențele biologice de aptitudini între sexe.

Îmi place mult studiul efectuat de către psihologul Carol Dweck cu un grup de copii din clasa a 5-a. În cadrul unui test, fetele au obținut scoruri mai mari la fiecare subiect în raport cu băieții, însă au renunțat mai repede când s-au confruntat cu o întrebare din test în afara nivelului lor de abilități. La fel în cadrul studiului s-a observat că băieții depun un efort mai sporit atunci când se confruntă cu adversitate. Interesant este că studiul a mai constatat că, cu cât IQ-ul unei fete este mai mare, cu atât probabilitatea e mai mare ca ea să renunțe la o întrebare din test. Consider că această diferență de atitudine – acest comportament prea precaut, cu risc scăzut – este fundamentală pentru dezechilibrul de gen în domeniul tehnologiei.

Ceea ce am dorit să emit ca mesaj cheie în cele spune mai sus este că noi „femeile" trebuie să ne recreăm ca abordare față de societate şi stilul de viață. Este necesar de a încuraja interesul femeilor pentru o carieră legată de domeniul tehnologiei la o vârstă mai fragedă, întru a educa calitățile şi aptitudinile necesare în acest sens.

9. Deci, care sunt primii pași pe care cineva îi poate face pentru a-și începe drumul către o carieră în securitatea cibernetică?

Sfatul meu pentru toată lumea este să vă urmați curiozitatea. Rămâneți precoce. Explorați și căutați comunități care să vă împărtășească pasiunea și interesul. Unul dintre lucrurile care ajută femeile și oamenii, în general, este găsirea devreme a spiritelor înrudite, adică să aderați la acele comunități sociale, profesionale care să vă motiveze şi încurajeze zi de zi.

10. Care sunt cărțile, blog-urile sau canalele YouTube de Tech și Securitate Cibernetică pe care le-ati recomanda celor interesați de aceste subiecte?

Următoarele cărţi recomand:

- Arta războiului de Sun Tzu,
- Dosar permanent de Edward Snowden,
- The Art of Active Defense,
- How to Lead When You're Not in Charge,
- Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon,
- This is how they tell me the world ends,
- Sandworm,
- Spam Nation.

Surse utile: https://www.cisecurity.org/, https://cve.mitre.org/, etc.

Larisa Găbudeanu

Șef Departament Securitate Informatică-CISO

1.Ce v-a atras inițial către domeniul securității cibernetice și cum v-ați dezvoltat cariera în acest domeniu?

La momentul când am finalizat studiile universitare în domeniul informatic, un domeniu care prezenta interes pentru mine era cel al securității cibernetice. Însă, având în vedere nivelul de dezvoltare scăzut al acestui domeniu la acel moment, nu am urmat un parcurs în domeniul securității cibernetice de la început. După aproximativ un deceniu într-un alt domeniu am revenit la domeniul securității cibernetice încet-încet. Mai întâi am urmat un master în domeniul securității cibernetice la Facultatea de Cibernetică din cadrul ASE București. Apoi am urmat cursuri și am obținut certificări în domeniul, implicându-mă în activități, evenimente și asociații în domeniu. Am continuat aceste activități și după schimbarea domeniului de activitate, activând în zona de securitate cibernetică.

2. Care a fost cea mai mare provocare pe care ați întâmpinat-o ca femeie în domeniul securității cibernetice și cum ați depășit-o?

Întrucât domeniul securității cibernetice este un domeniu în care activez după ce am avut o experiență de un deceniu într-un alt domeniu, pentru anumite aspecte a fost necesar un efort suplimentar pentru a înțelege contextul tehnic. Astfel, pentru a depăși această situație, am început prin acumularea cunoștințelor necesare prin aprofundarea subiectului în analiză.

3. Care sunt câteva dintre realizările de care sunteți cea mai mândră în cariera dvs. în securitatea cibernetică?

Sunt multe aspecte care îmi oferă satisfacție în activitatea mea. Printre momente importante aș putea menționa finalizarea cu succes a unor proiecte complexe cu privire la aspecte de noutate tehnologică pentru care nu era o standardizare în abordare din punct de vedere al securității cibernetice.

De asemenea, faptul că am contribuit la dezvoltarea persoanelor din echipă în profesioniști cu experiență în domeniul securității cibernetice reprezintă o mare satisfacție pentru mine.

4. Ce sfaturi aveți pentru femeile interesate de a-și urma o carieră în securitatea cibernetică și cum să-și depășească eventualele obstacole?

Consider că pentru a merge în direcția implicării în zona de securitate cibernetică este esențială identificarea domeniului de securitate cibernetică de interes. Desigur, este importantă și o înțelegere de ansamblu pentru a identifica consecințele anumitor amenințări și acțiuni de apărare a resurselor informatice.

De asemenea, pentru a asimila aspectele legate de securitatea cibernetică, pe lângă cursuri specifice pe anumite subiecte, citirea știrilor în domeniu și participarea la evenimente / comunități / asociații în domeniu sunt esențiale. Se regăsesc astfel de exemple atât a nivel național, în persoană sau online, precum și la nivel internațional, în mediul online.

5. Cum puteți încuraja și inspira alte femei să se implice în domeniul securității cibernetice?

Pentru a avea activitate într-un anumit domeniu consider importantă pasiunea pentru domeniul respectiv, timp dedicat cunoașterii domeniului și comunității aferente. În cadrul acestei comunități, prin proiecte dedicate sau nu, recomand găsirea unui mentor pentru a ghida procesul de inițiere în securitatea cibernetică.

Din punct de vedere al cunoașterii domeniului, recomand cursuri de introducere în securitate cibernetică pentru a acoperi elementele fundamentale din majoritatea domeniilor de securitate cibernetică si apoi o specializare într-un anumit domeniu. Cursurile interactive, cu elemente de gamification pot ajuta la aprofundarea și consolidarea anumitor concepte și principii.

6. Cum vedeți evoluția rolului femeilor în securitatea cibernetică în viitor și care sunt provocările și oportunitățile pe care le observați?

În domeniile securității cibernetice consider că femeile pot avea orice rol își doresc. Important este să aibă oportunitate de a explora domeniile aferente

securității cibernetice pentru a identifica dacă sunt domenii de interes pentru aprofundare sau pentru desfășurarea activității în viitor.

Astfel, este esențial ca activitățile privind cunoașterea domeniilor de securitate cibernetică, fie ele cursuri, workshop-uri, concursuri, burse, internship-uri, evenimente, să aibă ca destinatari și femeile. Pentru aceasta consider oportună o căutare activă a femeilor care au interes în domeniu pentru a fi invitate să participe la astfel de activități și ghidarea prin mentorat cu privire la opțiunile existente.

De asemenea, în cadrul organizațiilor, un accent pe echilibrarea echipelor prin includerea femeilor în cadrul acestora și prin includerea femeilor în zona de management, poate fi o altă abordare, în funcție de decizia fiecărei organizații în acest sens.

7. Care sunt cele mai valoroase abilități și competențe pe care le considerați necesare pentru succesul în domeniul securității cibernetice?

Consider că adaptabilitatea, integritatea și capacitatea de a rămâne calm în situații de criză/presiune sunt abilități esențiale pentru domeniul securității cibernetice.

Adaptabilitatea este esențială în majoritatea domeniilor în prezent, însă, în special în domeniul securității cibernetice având în vedere schimbările rapide necesare în structura și abordarea apărării resurselor informatice.

Integritatea este importantă și în acest domeniu, având în vedere necesitatea garantării identificării legislației și bunelor practici necesare și implementarea acestora corespunzător.

Capacitate de a rămâne calm în orice condiții este esențială având în vedere situațiile de investigare a potențialelor incidente de securitate.

8. Cum puteți folosi experiența și cunoștințele dvs. în securitatea cibernetică pentru a inspira și ajuta alte femei să-și urmeze pasiunea în acest domeniu?

Am încercat să contribui la creșterea numărului femeilor în acest domeniu prin realizarea de proiecte în care sunt implicate femei la început de drum în zona de securitate cibernetică, precum si prin acțiuni de coaching 1:1. Consider că

acțiunile de acest tip pot ajuta la creșterea comunității de femei din zona de securitatea cibernetică.

9. Ce vă motivează să continuați să lucrați în securitatea cibernetică și care este viziunea dvs. pentru viitorul femeilor din acest domeniu?

Ceea ce mă motivează este dinamica domeniului. Fiind în continuare mișcare atât zona de amenințări și tipologii de atac cibernetic, precum și cea de apărare a resurselor informatice, domeniul securității cibernetice presupune o activitate dinamică de continuă pregătire și continuă ajustare a metodelor de construire a apărării resurselor informatice.

Este un domeniu activ în care femeile pot evolua din punct de vedere profesional și personal, în funcție de preferințele lor cu privire la activitatea din domeniu și concentrarea pentru a aprofunda acest domeniu. Desigur, pentru a ajunge la o astfel de creștere a numărului de femei din domeniu, sunt necesare anumite activități pentru a aduce femei în acest domeniu, precum și pentru a ghida femei în evoluția lor, în special din partea femeilor care activează deja în zona securității cibernetice.

10.Toți oamenii pasionați de activitatea lor profesională au o parte favorită. Care e procesul de care vă simțiți cel mai atașat?

Domeniul securității cibernetice este unul extrem de vast, de la informațiile privind amenințările cibernetice, analiza alertelor de securitate, teste de penetrare și până la zona de guvernanță și gestionare a riscului. Fiecare din aceste zone presupun un anumit set de cunoștințe și abilități, precum și un anumit set de activități zilnice.

Aspectele de care mă simt atașată în activitatea mea sunt cele legate de implementarea și/sau ajustarea de procese interne pentru eficientizarea lor sau pentru implementarea unor cerințe de securitate noi (reieșite din bune practice sau din legislația relevantă în domeniu).

Astfel, pot menționa că zona de guvernanță, gestionarea riscului si conformitate sunt cele de care mă simt atașată.

Cristina Sucner

Inginer Integrare și servicii VAS

1. Ce v-a atras inițial către domeniul securităţii cibernetice și cum v-ați dezvoltat cariera în acest domeniu?

Domeniul IT cu care am făcut cunoştinţă acum 16 ani era un domeniu relativ nou care implica multe provocări interesante în activitatea zilnică și era şi rămâne un domeniu care e în permanenţă schimbare. Aceste două componente m-au captivat de la prima întâlnire. Una din provocările mele preferate este să găseşti soluţia unei probleme când eşti restrâns de timp, e adrenalină pură când cauţi motivul erorii prin informaţia care apare necontenit pe ecran.

2. Care a fost cea mai mare provocare pe care ați întâmpinat-o ca femeie în domeniul securității cibernetice și cum ați depășit-o?

Cea mai mare provocare cu care m-am întâlnit era neîncrederea celorlalţi precum că eu fiind femeie voi putea face faţă provocărilor zilnice. Se făceau glume de genul că nu voi putea face faţă lucrărilor de noapte căci prinţesele trebuie să-şi menţină regimul de somn ca să arate bine. Împreună cu solicitările colegilor primeam și partea de code care trebuia executată, la solicitările de implicare în proiecte interesante și primeam răspuns „Tu nu ai nevoie de asta,întrucât presupune să te trezeşti nopţile, în permanenţă să fii supusă stresului, la sigur nu ai nevoie de asta”. Partea complicată în astfel de situaţii e să nu le consideri din start adevăruri pure, e doar o părere a unui om care încă nu te cunoaşte. Astfel poziţionându-mă, am continuat să lucrez livrând în timp produse calitative, căutând soluţii de optimizare până când au făcut cunoştinţă toţi colegii mei cu mine.

3. Care sunt câteva din realizările de care sunteți cea mai mândră în cariera dvs. în securitatea cibernetică?

Sunt multe proiecte pe care mi le amintesc cu drag. Le voi specifica trei din ele care la momentul creării lor au adus automatizare, performanță şi inovaţie. În proiectul de automatizare creasem posibilitatea automată de arhivare digitală

a fişierelor scanate. Al doilea proiect în care am fost implicată a constat în creşterea performanţei serviciilor oferite clienţilor şi aici am lucrat 8 luni în crearea rapoartelor, analizei de date, identificarea KPI-urilor astfel corectând direcţia de creştere a performanţei. Al treilea proiect în care am avut ocazia să particip este implementarea eSIM. Acesta a adus atât libertatea în utilizare cât şi inovaţia mai aproape de clienţi.

4. Ce sfaturi aveți pentru femeile interesate de a-și urma o carieră în securitatea cibernetică și cum să-și depășească eventualele obstacole?

Pentru început, identifică cunoștințele care sunt necesare să le posezi ca să poţi începe o carieră în IT. Aici poţi utiliza site-urile cu anunţuri despre posturi disponibile și sub fiecare job oferit o să găseşti o listă de cerinţe pe care e necesar să le deţii.

Pasul doi ar fi sa găseşti cursuri care îţi pot completa aceste cunoștinţe. Ele pot fi atât online cât şi offline. Important este că primul curs ar trebui să fie unul general care îţi va contura domeniul şi direcţiile lui apoi poţi urma cursuri specializate per poziţia identificată. Pasul trei este să practici cele învăţate fie printr-un internship fie prin angajare directă pe poziţie de junior (începător).

Pasul următor este să te asiguri că menţii la zi cunoştinţele tale. De aceea identifici grupuri, newsletters, comunităţi şi evenimente care îţi pot fi utile în dezvoltarea ta. Ca să poţi trece prin toţi aceşti paşi e important să continui chiar dacă pare că înveţi chineza fără dicţionar, e nevoie de timp şi obişnuinţă cu termenii din domeniu şi de răbdare în parcursul devenirii unui specialist. Nu e o acţiune unică, e un proces repetitiv.

5. Cum puteți încuraja și inspira alte femei să se implice în domeniul securității cibernetice?

Cel mai greu moment în alegerea domeniului IT este să accepți să te aventurezi în el. Cel mai des motiv de stagnare în luarea unei astfel de decizii este neîncrederea în propria reuşită. Destul de des sunt întrebată ce va fi dacă nu voi reuşi?! Răspunzând la întrebarea aceasta de obicei spun că vei acumula cunoştinţe noi şi vei trăi liniştită că ai încercat, ai văzut cum este și nu a rămas doar o dorinţă neîmplinită care te macină în zilele complicate şi le întreb pe fete înapoi ce se va întâmpla dacă reuşeşti?! Acordând această întrebare deseori observ cum faţa persoanei cu care discut se luminează, atrage curajul şi porneşte în aventura cunoaşterii.

6. Cum vedeți evoluția rolului femeilor în securitatea cibernetică în viitor și care sunt provocările și oportunitățile pe care le observați?

În viitor văd o egalare între femei și bărbați pe aceleaşi roluri, fiecare în drept să-şi aleagă ce îl captivează şi îl motivează să se trezească în fiecare dimineaţă. Acţiuni care ar duce la egalarea rolului femeii vin din educaţia primită acasă sau în mediul social în care îşi petrece timpul în care respectarea alegerii făcute de femeie joacă un rol important în dezvoltarea ei ulterioară.

7. Care sunt cele mai valoroase abilități și competențe pe care le considerați necesare pentru succesul în domeniul securității cibernetice?

O abilitate importantă este să vezi situaţia multi-dimensional, să înțelegi de unde începe şi cu ce se finalizează procesul pe care îl analizezi, astfel eviţi interpretarea şi erorile ulterioare. O altă latură importantă este capacitatea de a interacţiona eficient cu echipa de lucru. Aici e important de subliniat aşa abilităţi precum ascultarea colegilor, identificarea modalităţii de comunicare între membrii unei echipe astfel evitându-se blocajele în proiecte. Cea mai importantă abilitate care necesită dezvoltată este perseverenţa care te ajută să nu renunţi la scopul propus iniţial.

8. Cum puteți folosi experiența și cunoștințele dvs. în securitatea cibernetică pentru a inspira și ajuta alte femei să-și urmeze pasiunea în acest domeniu?

În ultimii 3 ani am împărtăşit experienţa mea cu mai multe femei din Moldova prin participarea în calitate de speaker la evenimente dedicate, prin organizarea de evenimente care ar dezvolta abilităţi necesare pentru un progres în IT și am mentorat peste 100 de persoane în programe de reconversie în IT.

9. Ce vă motivează să continuați să lucrați în securitatea cibernetică și care este viziunea dvs. pentru viitorul femeilor din acest domeniu?

Motivaţia mea sunt proiectele interesante în special cele în cadrul cărora tehnologiile utilizate sunt mai puţin cunoscute pentru mine asta sporindu-mi nivelul de interes de a implementa proiectul, plus îmi dă şi o valoare adăugătoare, aceasta fiind tehnologia învăţată.

10.Toți oamenii pasionați de activitatea lor profesională au o parte favorită. Care e procesul de care vă simțiți cel mai atașat?

Cea mai preferată parte a procesului de lucru este mutarea produsului creat din mediu de test unde doar echipa de lucru îl poate vedea în mediu de producţie unde este utilizat de toţi clienţii. Utilitatea produsului creat este punctul maxim de satisfacţie pentru un dezvoltator.

11. Care sunt cărțile, blog-urile sau canalele YouTube de Tech și Securitate Cibernetică pe care le-ați recomanda celor interesați de aceste subiecte?

Sursele de învăţare diferă de la o perioadă la alta, depinde de cunoştinţele pe care le dezvolţi la moment, eu am câteva recomandări:

1. Utilizează sursa oficială a tehnologiei pe care o studiezi ;
2. Ca să fii la zi cu înţelegerea tehnologiilor care apar urmăresc TechWorld with Nana;
3. Pentru training-uri din domeniu folosesc udemy.com;
4. Pentru optimizări, clean code și refactoring urmăresc canalul Craft Software with Victor Rentea;
5. Pentru o experienţă cât mai variată participarea la evenimentele din domeniu.

Siguranța digitală începe cu tine

www.sigurantadigitala.md

Siguranță Digitală .md

eGA.ee

EU-Moldova Stronger Together

Siguranța digitală începe cu tine

Curs online - Protejează-te în mediul online

Un necunoscut începe să te urmărească pe stradă. Ar trebui să te împrietenești cu el? Un necunoscut vrea să te adauge în lista de prieteni pe Facebook. Ar trebui să te împrietenești cu el?

În era digitală de astăzi, prezența noastră online este strâns legată de experiențele noastre din viața reală.

Criminalitatea cibernetică a devenit cea mai răspândită infracțiune din lume, afectând persoane de toate vârstele, naționalitățile și nivelurile de educație. Protejarea lumii noastre digitale este esențială pentru a asigura securitatea noastră și a celor dragi și pentru a evita potențialele prejudicii.

Investind timpul dvs. în dezvoltarea competențelor esențiale în domeniul securității digitale, puteți reduce vulnerabilitatea la amenințările cibernetice și puteți profita la maximum de numeroasele oportunități pe care le oferă lumea digitală.

Nu pierdeți timpul — începeți acum! Preluați controlul asupra siguranței dvs. online! Urmează cursul nostru online și află cum să îți folosești smartphone-ul și computerul în siguranță!

Campania „SigurantaDigitala.md" este organizată de Proiectul "Asistență Rapidă în domeniul Securității Cibernetice pentru Republica Moldova" (finanțat de Uniunea Europeană) și ATIC. Campania și cursul online fac parte dintr-o misiune mai amplă de a crește gradul de conștientizare cu privire la securitatea cibernetică și de a oferi competențe digitale relevante în Republica Moldova.

www.sigurantadigitala.md

Parteneri

INSTITUTE FOR
WAR & PEACE REPORTING

IWPR (Institutul pentru Raportare despre Război și Pace)

Institutul pentru Raportare despre Război și Pace (iwpr.net) este o organizație internațională non-profit cu sediul central în Londra și Washington DC. IWPR promovează pacea și democrația prin sprijinirea mass-mediei libere și corecte, consolidează mass-media locală în primele linii ale conflictelor și schimbării, activând în peste 30 de țări și regiuni din lume. Activitatea IWPR include crearea mass-mediei locale independente, instruiri pentru reporteri, editori și producători locali, sprijin pentru informarea extinsă și aprofundată în domenii ce țin de drepturile omului, buna guvernare și alte aspecte aferente, promovarea informării profesioniste în țările în curs de dezvoltare și la nivel internațional și consolidarea capacităților de comunicare ale organizațiilor locale din domeniul drepturilor omului, justiției internaționale și ale organizațiilor conduse de femei.

e-Governance Academy (eGA)

e-Governance Academy (eGA) este o organizație de consultanță și un grup de reflecție non-profit care asistă organizațiile din sectorul public și din societatea civilă în realizarea transformării digitale. eGA oferă servicii de consultanță în domeniul guvernării electronice și al gestionării transformărilor, vizite de studiu, cursuri de formare și conferințe în Estonia și în străinătate din 2002. Până în prezent, eGA a cooperat cu peste 280 de organizații și a instruit peste 9 000 de funcționari din 140 de țări și regiuni. eGA are în componență 75 de experți și membri ai personalului pentru a asigura disponibilitatea unei expertize globale de vârf pentru toți partenerii noștri. Peste 300 de experți în e-guvernare sunt implicați în rețeaua globală de competențe a eGA. Toți aceștia au o experiență practică unică în dezvoltarea de soluții de e-guvernare și o experiență îndelungată în managementul schimbării în sectorul public.

eGA a obținut un certificat ISO 9001:2015 în domeniul managementului de proiect, al formării și consultanței în domeniul e-guvernării.

eGA conduce proiectul de Asistență Rapidă în domeniul securității cibernetice în Moldova, al cărui obiectiv general este de a spori reziliența cibernetică a organizațiilor din sectorul public și a sectoarelor cheie de infrastructură critică. Experții eGA lucrează în Moldova pentru a intensifica consolidarea capacităților părților interesate din Moldova, pentru a le permite acestora să elaboreze cadrele juridice ale instituțiilor de securitate cibernetică și pentru a le alinia la strategia, standardele și cadrul juridic și politic relevant al UE, în special, dar nu numai, la Directiva NIS.