UNIUNEA EUROPEANĂ
Fondul Social European

GUVERNUL ROMÂNIEI
Ministerul Dezvoltării Regionale
și Administrației Publice

Inovație în administrație
Programul Operațional
"Dezvoltarea Capacității
Administrative"

Proiect: Sistemul Național de Combatere a Criminalității Informatice „Cyber Crime"
Cod SMIS: 37595

Beneficiar:
Centrul Național de Răspuns la Incidente de Securitate Cibernetică CERT-RO

Set propuneri de politici publice în vederea combaterii criminalității informatice și îmbunătățirii climatului de securitate cibernetică în România

Proiect cofinanțat din Fondul Social European prin
Programul Operațional Dezvoltarea Capacității Administrative 2007-2013

Soluții reale pentru amenințări virtuale

www.cert-ro.eu

Propunere de politică publică privind extinderea Sistemului de Alertă Timpurie („SAT")

Formularea problemei:

Principalele probleme întâmpinate de CERT-RO în operarea SAT sunt următoarele:

- **Nu primește în mod sistematic alerte de la organizații de drept public sau privat** din România, pentru că nu există obligativitate de raportare în sarcina acestora;
- **Majoritatea informațiilor provin de la organizații din exterior** care solicită rezolvarea unor probleme punctuale ce provin de la adrese IP din România;
- **Atunci când CERT-RO solicită informații către organizațiile menționate, nu primește întotdeauna răspuns**, deoarece nu există o obligativitate în acest sens în sarcina respectivelor organizații.

Obiective specifice:

- **Definirea cuprinzătoare a categoriilor de actori care trebuie responsabilizați**
- **Clarificarea responsabilităților, abilităților și capabilităților** pe componenta de alertare
- **Identificarea măsurilor legislative, instituționale, tehnice, procedurale și de cooperare** internațională necesare în vederea eficientizării sistemului de alertare.

Varianta propusă:

Consolidarea instituțională a CERT-RO și reglementarea relațiilor acesteia cu entitățile din mediul public și privat din România prin:

1. **Extinderea/clarificarea mandatului CERT-RO**, prin adăugarea unor noi atribuții sau detalierea celor existente, pentru a cuprinde următoarele competențe:
   - Impunerea unor măsuri obligatorii de securitate în sarcina entităților vizate;
   - Solicitarea către entitățile vizate a (i) furnizării către CERT-RO a informațiilor necesare și politicilor de securitate aplicabile, în vederea evaluării securității infrastructurilor acestor entități; (ii) supunerii respectivelor entități unui audit de securitate și transmiterii concluziilor acestuia către CERT-RO;

   - Investigarea situațiilor de potențială încălcare a obligațiilor privind (i) introducerea unor norme și proceduri de securitate minimale obligatorii și (ii) colaborarea cu CERT-RO și sancționarea acestor entități, dacă este cazul.

2. **Introducerea unor obligații pentru entitățile vizate**, eventual în mod proporțional cu gradul de risc al acestora din punct de vedere al securității cibernetice, care să includă următoarele:
   - Raportarea incidentelor de securitate cibernetică;
   - Crearea de structuri de tip CERT organizaționale. CERT-RO va menține un registru al structurilor de tip CERT care raportează către CERT-RO asemenea incidente;
   - Crearea de structuri CERT sectoriale care să preia alertele entităților dintr-un anumit sector (telecom, financiar bancar, etc), să le centralizeze și să le transmită către CERT-RO
   - În cazul în care CERT-RO decide, în urma parcurgerii etapelor legale, că incidentele de securitate sunt de interes public, (i) informarea publicului la solicitarea CERT-RO cu privire la aceste incidente sau (ii) acceptul și/sau cooperarea la informarea publicului de către CERT-RO în acest sens, opțiunea între (i) și (ii) urmând să revină CERT-RO.

2. **Asigurarea necesarului de personal și logistic necesar și a unui buget corespunzător** pentru îndeplinirea de către CERT-RO a mandatului său extins.

Propunere de politică publică privind definirea statutului de furnizor de servicii de securitate cibernetică în vederea dezvoltării capacității de răspuns la incidentele de securitate

Scop:

Stabilirea acțiunilor necesare în vederea stabilirii statutului și a condițiilor de funcționare a furnizorilor de servicii de securitate cibernetică.

Obiective specifice:

- Definirea statutului de furnizor de servicii de securitate cibernetică și crearea cadrului legal necesar pentru funcționarea furnizorilor de servicii de securitate cibernetică
- Stimularea organizațiilor pentru a realiza investiții în vederea furnizării de servicii de securitate cibernetică
- Stimularea organizațiilor pentru a dezvolta produse de securitate cibernetică

Varianta propusă:

Consolidarea instituțională a CERT-RO prin extinderea/clarificarea mandatului CERT-RO, prin adăugarea atribuției de menținere a unui Registru al Furnizorilor de securitate cibernetică.
Registrul va defini și principalele categorii de servicii de securitate cibernetică:

- Servicii de monitorizare a securității sistemelor informatice
- Servicii de management al incidentelor de securitate de către o structura de tip CERT
- Servicii de administrare a securității sistemelor informatice
- Servicii de testare și audit a securității sistemelor informatice
- Servicii de evaluare a securității produselor ICT și a produselor de securitate cibernetică

Înscrierea în acest Registru a furnizorilor va fi voluntară. Dacă un anumit furnizor nu este prezent în acest Registru nu înseamnă ca nu va putea furniza astfel de servicii.

Furnizorii înscriși în Registru, vor fi verificați și aprobați în cadrul unui proces de certificare gestionat de CERT-RO, pe baza unei Metodologii și a unor criterii, specifice serviciilor pe care le furnizează solicitanții, respectiv produselor în funcție de o serie de cerințe specifice minimale.

În vederea stimulării înscrierii furnizorilor în registru se propune acordarea de facilități care să le permită întreținerea și optimizarea sistemelor, astfel:

- Cheltuielile efectuate pentru investiții, dotări și alte utilități necesare desfășurării activității de oferire a serviciilor de securitate cibernetică se scad din veniturile brute, pe o durată de 2 ani de la începerea acestei activități.
- Cheltuielile pentru modificarea și perfecționarea sistemelor informatice utilizate pentru oferirea serviciilor de securitate cibernetică se scad din veniturile impozabile aferente anului fiscal în care s-a efectuat investiția.

De asemenea, pentru a stimula organizațiile naționale să dezvolte produse de securitate cibernetică se va avea în vedere scutirea de impozit pentru profitul reinvestit în dezvoltarea acestui tip de produse.

Propunere de politică publică privind înființarea și operaționalizarea unei unități specializate de tip "Patrulă cibernetică"

Scop:

Creșterea capacității instituționale a Poliției Române de investigare a faptelor penale din sfera criminalității informatice.

Obiective specifice:

Crearea și operaționalizarea în cadrul Serviciului de Combatere a Criminalității Informatice unei structuri de tip „Patrula Cibernetică", care să fie în măsură să:

- obțină informații privind iminența ori posibilitatea săvârșirii de infracțiuni prin prezența în mediul online (forum-uri, grupuri de discuții, camere de chat etc.);
- analizeze resursele web existente în spațiul cibernetic public, în căutarea de conținut ilegal;

- fie prezente în rețele de tip P2P și File Sharing (în căutare de conținut ilegal, identificarea transferurilor de materiale pornografice cu minori sau cu încălcarea drepturilor de autor etc.)
- verifice legalitatea tranzacțiilor comerciale desfășurate prin Internet (comerț electronic);
- identifice din timp și să studieze posibilii infractori, prin verificarea mediilor virtuale de socializare a persoanelor care manifestă preocupări evidente pe linia comiterii de infracțiuni informatice cum ar fi atacuri cibernetice, exploatării de vulnerabilități ale platformelor IT&C etc. („subterană digitală").
- identifice noi trenduri/moduri de operare ale grupărilor specializate în comiterea de infracțiuni contra sistemelor informatice sau cu mijloace de plată electronică.

Varianta propusă:

Înființarea și operaționalizarea unei unități pilot de Patrulă Cibernetică în cadrul Serviciului de Combatere a Criminalității Informatice, care să-și desfășoare activitatea în cadrul procedural existent;

Stabilirea mandatului și a procedurilor de lucru ale unității;

Stabilirea și asigurarea necesarului de resurse umane și logistice pentru desfășurarea în condiții optime a mandatului;

Asigurarea pregătirii specifice a membrilor unității;

Operaționalizarea unității și interconectarea ei prin protocoale de colaborare cu entitățile principale cu care interacționează conform mandatului;

Utilizarea experienței acumulate pentru:

- stabilirea necesităților de modificări legislative pentru extinderea mandatului unității
- crearea planurilor și instrucțiunilor de exindere a unității funcție de necesități.

Propunere de politică publică privind formarea de juriști cu specializare în domeniile drept informatic, probe digitale și criminalitate informatică

Formularea problemei:

În prezent, în țară numărul de cursuri în cadrul instituțiilor de învățământ superior care să abordeze integrat problematica enunțată (drept informatic, probe digitale, criminalitate informatică), într-o manieră care să ofere competențe de bază juriștilor sau opțiuni de specializare a acestora în domeniile vizate este extrem de mic.

Scop:

Stabilirea acțiunilor necesare la nivel guvernamental în vederea creșterii numărului de juriști și specialiști (judecători, procurori, polițiști, avocați, consilieri juridici) cu specializare pe domeniile: dreptul tehnologiei informației (sau drept informatic), criminalitate informatică și probe digitale.

Obiective specifice:

- Formarea de competențe pe domeniul drept informatic și criminalitate informatică pentru specialiștii implicați în cercetarea și judecarea (judecători, procurori, polițiști, avocați, etc.) faptelor din acest domeniu.
- Formarea de competențe pe domeniul probelor digitale pentru specialiștii în drept în general.
- Crearea de oportunități de specializare pe domeniile vizate pentru absolvenții de învățământ superior.

Varianta propusă:

Adresarea generală a problemei prin formarea în cadrul învățământului post-universitar (masterat, doctorat) în științe juridice, a competențelor de bază și specializărilor privind probele digitale, dreptul IT și criminalitate informatică prin:

1. **introducerea în curicula de pregătire post universitară a unor module obligatorii** de specializare în Drept informatic, probe digitale și criminalitate informatică pentru un set prestabilit de studii universitare de masterat și doctorat ori programe de cercetare post-doctorală sau postuniversitare în drept (ex.: Științe Penale, Drept Financiar, Drept Bancar și al Asigurărilor, Administrație Publică, Poliție, etc.)

2. introducerea unor module speciale de drept informatic, criminalitate informatică și probe digitale în programa cursurilor de **master în securitatea informației** (după modelul Academiei Tehnice Militare)

Avantaje:

- Asigură pe termen lung formarea de competențe pe cele două domenii
- Permite statului să aloce de la buget sume doar pentru formarea avansată de specialiști în domeniu.

Dezavantaje:

- Numărul în prezent scăzut de cadre didactice pregătite și titularizate care să susțină aceste cursuri, ținând cont de specificitatea disciplinelor și abundența de noțiuni tehnice, competența fiind dublu condiționată: drept și IT.

Propunere de politică publică privind formarea inițială și pregătirea profesională continuă a procurorilor și judecătorilor în domeniile: drept informatic, probe digitale și criminalitate informatică

Formularea problemei:

Pregătirea adecvată sub aspectul înțelegerii noțiunilor și fenomenelor tehnice cât și a semnificației lor în plan juridic atât pentru magistrații și personalul asimilat din instituțiile de aplicare a legii implicate în cercetarea cauzelor penale din sfera criminalității informatice cât și de către judecătorii și procurorii implicați în judecarea cauzelor la instanță reprezintă o condiție esențială pentru aducerea în justiție a faptelor penale din sfera criminalității informatice și a actelor civile și comerciale legate de mediul cibernetic.

Scop:

Stabilirea acțiunilor necesare la nivel guvernamental în vederea creșterii numărului de magistrați cu pregătire în domeniile: drept informatic, probe digitale și criminalitate informatică.

Obiective specifice:

- Formarea de competențe pe domeniul criminalității informatice pentru magistrații implicați în actul de justiție (judecători, procurori, avocați, forțe de ordine, etc.) privind faptele de criminalitate informatică;
- Formarea de competențe pe domeniul probelor digitale pentru magistrați;
- Stabilirea de parteneriate de tip public-privat și includerea în lista formatorilor agreați a unor specialiști din mediul academic, companii din domeniul securității cibernetice, CERT-RO, instituții de aplicare a legii sau centre de studiu pe tematica de interes vizată.

Varianta propusă:

Adresarea problemei prin introducerea pregătirii inițiale obligatorii (cursuri în cadrul I.N.M.) precum și prin introducerea în programa de pregătire profesională continuă a magistraților aflați în funcție, de conținuturi care să le confere competențele necesare în cauzele ce implică drept informatic, probe digitale și criminalitate informatică, astfel:

Formare inițială pentru auditorii de justiție

1. introducerea în programa obligatorie de formare din cadrul Institutului Național al Magistraturii a noțiunilor privitoare la dreptul IT, criminalitatea informatică și probele digitale.

Formare continuă pentru magistrații în funcție

2. introducerea în cadrul stagiilor de pregătire profesională continuă obligatorie a magistraților a noțiunilor privitoare la dreptul informatic, criminalitatea informatică și probele digitale
3. stabilirea de parteneriate public-privat și includerea în lista formatorilor agreați a unor specialiști din mediul academic, companii din domeniul securității cibernetice, CERT-RO, instituții de aplicare a legii sau centre de studiu pe tematica de interes vizată.
4. prioritizarea participării la seminarii în domeniu organizate în străinătate (Academy of European Law (ERA), European Judicial Training Network (EJTN), European Police College (CEPOL), etc.)

Propunere de politică publică privind formarea inițială și pregătirea profesională continuă a polițiștilor în drept informatic, criminalitate informatică și probe/investigații digitale

Formularea problemei:

Una dintre cele mai dificile provocări pentru aceste structuri ale Poliției Române este adaptarea continuă la noile scheme infracționale și la noile tehnologii folosite de către infractorii cibernetici. În acest context, activitățile de pregătire profesională sunt extrem de importante, ele reflectându-se în capacitatea de combatere a acestui fenomen.

Scop:

Stabilirea acțiunilor necesare la nivel guvernamental în vederea formării profesionale și a creșterii nivelului de instruire, competență și expertiză al tuturor polițiștilor care își desfășoară activitatea în cadrul unităților specializate de combatere a criminalității informatice.

Obiective specifice:

- Formarea de competențe pe domeniul criminalității informatice pentru structurile specializate ale Poliției Române.
- Conceperea și punerea în aplicare de programe și mecanisme pe termen lung de asigurare a numărului necesar de polițiști instruiți pe domeniile vizate.
- Conceperea de programe și proceduri periodice care să asigure adaptarea continuă a structurilor Poliției Române la noile scheme infracționale și la noile tehnologii folosite de către infractorii cibernetici.
- Instituirea de parteneriate public-privat pentru asigurarea de resurse atât financiare cât și umane pentru pregătire și formare.

Varianta propusă:

Adresarea globală a problemei prin introducerea pregătirii inițiale obligatorii (în cursul formării) precum și prin introducerea în programa de pregătire profesională continuă a elementelor necesare care să confere competențele de bază necesare.

Introducerea la recomandarea IGPR în cadrul planurilor de învățământ de la forma de studii universitare licență organizată în Academia de Poliție a unor discipline specializate de drept informatic, criminalitate informatică și probe digitale.

Identificarea de resurse bugetare permanente pentru formarea profesională în centrele specializate.

Identificarea și alocarea de resurse bugetare precum și atragerea de resurse extrabugetare pentru asigurarea continuității Centrului Roman de Excelență pentru Cybercrime - CYBEREX-RO după data finalizării proiectului.

Formarea de parteneriate public-privat pentru mobilizarea de resurse extrabugetare pentru instruire și includerea în lista formatorilor agreați a unor specialiști din mediul academic, companii din domeniul securității cibernetice, CERT-RO, sau centre de studiu pe tematica de interes vizată.

Propunere de politică publică privind instruirea specifică a judecătorilor, procurorilor și polițiștilor prin exerciții și simulări integrate pe domeniile securitate cibernetică și criminalitate informatică

Formularea problemei:

Pentru a crește eficiența și eficacitatea acțiunilor de combatere a infracționalității din domeniul informatic, personalul specializat din cadrul structurilor centrale și teritoriale ale Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism și ale Direcției de Combatere a Crimei Organizate din Inspectoratul General al Poliției Române trebuie să parcurgă o serie de etape de instruire specifică în domeniile drept IT, criminalitate informatică și probe digitale.

Ca orice proces de formare profesională ori de perfecționare, acesta nu ar trebui să se limiteze la obținerea de informații juridice sau tehnice (de altfel, absolut necesare), ci ar trebui să vizeze inclusiv partea practică, aplicativă, a cunoștințelor dobândite.

Scop:

Stabilirea acțiunilor necesare la nivel guvernamental în vederea organizării de exerciții și simulări de instruire specifică în domeniul combaterii criminalității informatice.

Obiective specifice:

- Formarea de abilități practice pe domeniul combaterii criminalității informatice pentru polițiști, procurori și judecători.

Varianta propusă:

Organizarea sub egida CERT-RO de exerciții și simulări integrate pe segmentul combaterii criminalității informatice în următoarele modalități:

1. Realizarea periodică de exerciții de securitate cibernetică la nivel național.
2. Lărgirea ariei de cuprindere a exercițiilor de securitate cibernetică organizate la nivel național, prin adăugarea unei extensii care să acopere procedural toate actele întreprinse de organele de cercetare penală, de la faza identificării sau notificării unui incident de securitate cibernetică cu suspiciune de faptă penală și până la obținerea tuturor probelor necesare întocmirii rechizitoriului și prezentarea acestuia în instanță.
3. Extinderea pe segmentul de aplicare a legii a exercițiilor de securitate cibernetică organizate și desfășurate de către Agenția Europeană pentru Securitatea Sistemelor și Rețelelor (ENISA), cu participarea tuturor entităților de tip CERT din Europa.
4. Participarea la exercițiile organizate de Uniunea Internațională a Telecomunicațiilor, de cooperare în domeniul combaterii criminalității informatice, pe modelul academic al sesiunilor Moot Court (sau Mock Court), prilej cu care instituțiile de aplicare a legii din diferite state schimbă informații și ghiduri de bune practici, simulând intervenția și cercetarea penală a unor infracțiuni informatice.

Propunere de politică publică privind definirea unui standard ocupațional și a unor criterii de competență de bază pentru personalul care operează și administrează infrastructuri de securitate informatică

Formularea problemei:

Clasificarea ocupațiilor din România nu conține poziții specifice pentru personalul care asigură securitatea informației.

Scop:

Stabilirea acțiunilor necesare la nivel guvernamental în vederea definirii unui standard ocupațional și a unor criterii de competența de bază pentru personalul care operează și administrează infrastructuri de securitate informatică.

Obiective specifice:

- Definirea unui standard ocupațional pentru Manager securitate informatică
- Definirea unui standard ocupațional pentru Administrator de securitate informatică
- Definirea unei structuri organizaționale subordonate Managerului securitate informatică
- Stabilirea unor fișe de clasificare și calificări de bază pentru personalul ce operează și administrează infrastructuri de securitate informatică
- Stabilirea unui program de formare pentru obținerea calificărilor de bază de către personalul ce operează și administrează infrastructuri de securitate informatică.

Varianta propusă:

Îmbunătățirea cadrului organizațional și definirea unor cerințe de calificare de bază pentru personalul care operează și administrează infrastructuri de securitate informatică prin:

- Definirea unui standard ocupațional pentru **Manager securitate informatică** prin actualizarea Structurii Clasificării Ocupațiilor din România. Managerul securitate informatică va fi diferit de CISO și se va situa în afara structurii IT a organizației infracțiuni informatice.

- Definirea unui standard ocupațional pentru **Administrator de securitate informatică** prin actualizarea Structurii Clasificării Ocupațiilor din România. Administratorul de securitate informatică va fi va avea funcția tehnică de monitorizare, administrare și configurare efectivă a echipamentelor și componentelor ce asigură securitatea cibernetică a organizației.
- Definirea unei structuri organizaționale subordonate Managerului securitate informatică, structură ce trebuie inclusă în organigrama entităților vizate
- Stabilirea unor fișe de clasificare și calificări de bază pentru personalul ce operează și administrează infrastructuri de securitate informatică
- Stabilirea unui program de formare pentru obținerea calificărilor de bază de către personalul ce operează și administrează infrastructuri de securitate informatică
- Formarea de parteneriate public-privat pentru mobilizarea de resurse extrabugetare pentru instruire și includerea în lista formatorilor agreați a unor specialiști din mediul academic, companii din domeniul securității cibernetice, CERT-RO, sau centre de studiu pe tematica de interes vizată.

Propunere de politică publică privind stabilirea unui program guvernamental de comunicare publică unitară în scopul prevenirii criminalității informatice

Formularea problemei:

În momentul de față se constată o conștientizare redusă în rândul publicului larg din Romania privind:

1. cunoașterea amenințărilor specifice spațiului cibernetic și înțelegerea riscurilor ce derivă din utilizarea sistemelor informatice, ori a mijloacelor electronice de comunicare;
2. cunoașterea și adoptarea unor măsuri tehnice minimale privind securitatea cibernetică, precum și protecția datelor personale;
3. adoptarea unui comportament personal adecvat și responsabil atât în utilizarea sistemelor informatice cât și în mediul online.

Totodată se constată o lipsă de cunoaștere de către utilizatorii finali a faptelor care constituie infracțiuni informatice, a consecințelor acestora atât pentru făptuitori cât și pentru victime (persoane fizice sau juridice), precum și a modului de a acționa în cazul în care cetățenii cad victime ale acestor tipuri de infracțiuni informatice.

Scop:

Stabilirea acțiunilor necesare la nivel guvernamental în vederea creșterii gradului de conștientizare în rândul populației privitor la:

- Amenințările specifice spațiului cibernetic;
- Securitatea cibernetică și măsurile de protecție minimale necesare;
- Infracțiunile din domeniul informatic;
- Modul de a solicita ajutorul statului în cazul în care o persoană sau entitate cade victimă acestui tip de infracționalitate.

Obiective specifice:

- Comunicarea pe înțelesul cetățenilor de informații la zi privind mijloacele tehnice de protecție în spațiul cibernetic, în vederea conștientizării problemelor create de programele software dăunătoare în domeniul financiar comerț electronic, mijloace de plată electronică;
- Comunicarea pe înțelesul cetățenilor a tipurilor de comportament necesar a fi adoptat în vederea creșterii gradului de siguranță în utilizarea sistemelor informatice și a internetului;
- Comunicarea către cetățeni a direcțiilor de acțiune pe care statul le pune la îndemâna lor în cazul în care aceștia cad victime criminalității informatice;
- Popularizarea campaniilor și programelor desfășurate de mediul public și privat pe domeniul prevenirii și combaterii criminalității informatice și a creșterii gradului de siguranță cibernetică;
- Explicitarea pe înțelesul cetățenilor a faptelor care intră în sfera infracțiunilor informatice.
- Explicarea consecințelor legale, materiale și sociale a comiterii de astfel de fapte;
- Popularizarea de statistici (lunar, trimestrial, semestrial, anual) privind criminalitatea informatică și incidentele de securitate;
- Popularizarea cazurilor de succes în identificarea, prinderea și trimiterea în justiție a infractorilor informatici;
- Oferirea de suport mediului public și celui privat pentru organizarea de campanii specifice de informare și conștientizare în rândul populației.

Varianta propusă:

- Stabilirea unui program guvernamental de comunicare publică în scopul prevenirii criminalității informatice, inițiat și derulat de un consorțiu alcătuit din MSI (CERT-RO), MAI-IGPR (DCCO), Ministerul Public (DIICOT) și SRI (Cyberint), Ministerul Educației Naționale.

- Acest consorțiu va stabili parteneriate cu mediul de afaceri, cu mediul academic, centre de cercetare în domeniul criminalității informatice și organizații neguvernamentale interesate pentru derularea în comun de programe de conștientizare adecvate diferitelor categorii de public țintă.
- Acest consorțiu va stabili parteneriate cu toate instituțiile media (posturi de radio și TV, locale și naționale, publicații online, agenții de știri etc.) pentru:
- Alocarea de timp (în cazul radio și TV) și spațiu (în cazul publicațiilor) pentru diseminarea de informații, mesaje, comunicate etc. referitoare la situații, stări, fapte sau acțiuni cu relevanță în domeniul prevenirii și combaterii criminalității informatice;
- Efectuarea de demersuri pe lângă Consiliul Național al Audiovizualului în vederea obținerii sprijinului legal pentru a determina posturile de radio și TV să difuzeze mesaje „de interes public" - referitoare la siguranța IT, pericolele specifice mediului virtual etc. (similar campaniilor derulate în trecut de IGP în cadrul Proiectului Safe Internet, cu deviza „Tu cui dai accept?")
- Realizarea, cu regularitate, în reviste de profil și nu numai, de interviuri cu personalități în domeniu (ex. profesioniști din cadrul agențiilor de aplicare a legii, CERT-RO, SRI sau alții, profesori, cercetători, experți din companii de securitate IT etc.);
- Crearea și lansarea de pagini Facebook și conturi de Twitter în vederea diseminării de informații și noutăți relevante în domeniu, precum și inter-relaționarea acestora cu platforme și inițiative private similare deja existente (ex. www.legi-internet.ro, www.criminalitate.info, www.criminalitate-informatica.ro etc.)
- Crearea unei aplicații mobile (pentru sisteme iOS, Android etc.) care să faciliteze accesul în Portalul Guvernamental de Prevenire și Combatere a Criminalității Informatice, în vederea obținerii de informații sau raportării de incidente.
- Comunicarea pe înțelesul cetățenilor a pericolelor/amenințărilor din mediul cibernetic si modul de a le evita.
- Crearea și Promovarea Portalului Guvernamental Unic de Prevenire și Combatere a Criminalității Informatice și a logo-ului acestuia (ce va fi creat) pe toate paginile instituțiilor cu atribuții în domeniul securității cibernetice, securității naționale, prevenirii și combaterii criminalității informatice și, opțional, pe paginile web ale autorităților publice centrale și locale interesate.
- Crearea în cadrul Platformei Electronice Unice de Informare și Consultanță în domeniul Criminalității Informatice, ca punct unic de suport informațional și spațiu de vehiculare a celor mai bune practici și soluții, atât juridice cât și tehnice, la dispoziția cetățenilor, mediului de afaceri, sectorului guvernamental etc.

Propunere de politică publică îmbunătățirea educației pentru elevi și studenți în domeniul securității IT și prevenirea criminalității informatice. Pregătirea de competențe în domeniu. Creșterea gradului de siguranță a utilizării tehnologiei informației în școli și universități

Formularea problemei:

În momentul de față, se constată lipsa unor instrumente și mecanisme eficiente de protecție a minorilor împotriva conținuturilor dăunătoare din spațiul virtual și a efectelor nedorite ale utilizării de către aceștia a Internetului. La nivel gimnazial, deși obligatorie conform legii, disciplina TIC nu este predata întrucât planul cadru nu a fost actualizat.

Scop:

Stabilirea acțiunilor necesare la nivel guvernamental în vederea creșterii siguranței utilizării tehnologiei informației de către copii și tineri.

Obiective specifice:

- Definirea cuprinzătoare a categoriilor de actori care trebuie responsabilizați și angrenați pe componenta de educație în domeniul securității IT - componentă esențială în procesul de prevenire a criminalității informatice -, incluzând autoritățile și instituțiile publice, furnizorii de servicii de acces la internet, furnizorii de servicii ale societății informaționale, furnizorii de educație - instituții din sistemul național de învățământ -, mediul academic, organizațiile neguvernamentale etc., în vederea educării copiilor și tinerilor pentru prevenirea victimizării acestora ca urmare a folosirii internetului;
- Dezvoltarea competențelor, abilităților și capabilităților copiilor și tinerilor privind utilizarea tehnologiei informației, precum și identificarea eventualelor situații favorizante săvârșirii de fapte specifice criminalității informatice;
- Identificarea măsurilor legislative, instituționale, tehnice și procedurale necesare în vederea creșterii gradului de siguranța a utilizării tehnologiei informației în sistemul național de învățământ, atât la nivelul universitar, cât și preuniversitar.

Varianta propusă:

Modificarea curriculei la nivelul învățământului preuniversitar și universitar prin:

- Introducerea în curricula școlară a disciplinei TIC de la nivelul învățământului primar, ca disciplină obligatorie.
- Dezvoltarea unei curricule integrate și adaptată pe etapele de vârstă și problemele specifice pentru fiecare etapă.
- Introducerea în programele de studiu (acolo unde există) de conținuturi privind securitatea online și siguranța în utilizarea IT, indiferent dacă TIC este disciplină obligatorie sau opțională și indiferent de nivel.
- Completarea sistemului de evaluare al ARACIP și ARACIS în concordanță cu noua curriculă.
- Programe de formare profesională dedicate cadrelor didactice implicate în activități care folosesc sistemele informatice, cu accent pe mijloacele și metodele de prevenire a criminalității informatice ce vizează copii.
- Pregătirea de competențe în domeniul securității IT prin introducerea în planurile de învățământ din învățământul superior a unei discipline specifice care să reprezinte o precondiție de acces la o funcție didactică din învățământul preuniversitar.
- modificarea art. 68 alin.(3) din Legea nr. 1/2011 a educației naționale în sensul: „Disciplina Tehnologia informației și comunicării constituie o disciplină ***obligatorie*** pentru elevii din învățământul preuniversitar";
- programele analitice ale disciplinei TIC sau similare, începând cu cele din învățământul preșcolar, să conțină teme privind securitatea online și siguranța în utilizarea IT adaptate vârstei celor cărora li se adresează;
- adaptarea programelor analitice ale disciplinelor studiate în cadrul formării inițiale și continue a cadrelor didactice cu accent pe mijloacele și metodele de prevenire a criminalității informatice ce vizează copii;
- modificarea planului cadru pentru anul școlar următor pentru a include disciplina TIC la nivel de gimnaziu
- instituirea curriculei propuse prin intermediul proiectului **„Competențe cheie TIC în curriculumul școlar"** ca obligatorie la nivel de gimnaziu.

Propunere de politică publică măsuri de protecție juridică a organizațiilor din mediul public și privat împotriva "amenințărilor din interior" privitoare la securitatea cibernetică

Formularea problemei:

Deși amenințările la adresa securității cibernetice sunt percepute în general ca venind din exteriorul entităților protejate, numeroase studii arată faptul că numeroase incidente ce au avut ca rezultat furtul de date și compromiterea de sisteme informatice, au avut drept cauză principală amenințările venite din interior, fie ele intenționate (angajați și funcționari rău intenționați, răzbunare, etc.), fie neintenționate (din necunoaștere).

Scop:

Măsuri de conștientizarea de către angajați și angajatori a necesității adoptării unor măsuri minimale privind securitatea cibernetică.

Obiective specifice:

- Crearea unui cadru juridic global de protecție împotriva amenințărilor la adresa securității cibernetice din interiorul organizațiilor
- Creșterea disciplinei la locul de muncă legat de infrastructura IT
- Opozabilitatea în justiție a relațiilor angajator-angajat în privința conduitei de urmat legată de utilizarea infrastructurii IT la locul de muncă
- Conștientizarea de către angajatori si angajați deopotrivă a necesității unei conduite orientate spre securitatea cibernetică la locul de muncă.
- Instruirea de bază a angajaților cu privire la conduita în utilizarea sistemelor informatice și a internetului la locul de muncă.

Varianta propusă:

Amendarea Codului Muncii, Art. 242 privitor la conținutul obligatoriu al Regulamentului Intern.

Introducerea în lista a unei noi dispoziții care să prevadă obligativitatea unei secțiuni din regulament dedicată specific modului de operare și conduitei de adoptat în lucrul cu date și sisteme informatice ori cu mijloace de comunicare electronice, în cadrul organizației, în interesul serviciului.

Instituirea de obligații către angajați trebuie să aibă corelativ pentru angajatori obligația de instruire minimală asupra conduite de urmat pentru creșterea gradului de securitate informatică.

Avantaje:

- Instituie o protecție juridică angajatorilor în relațiile de muncă privitoare la datele și sistemele informatice.
- Costuri minime pentru toate organizațiile pentru redactarea și adaugarea la Regulamentul Intern a unei noi prevederi.
- Conștientizarea atât de către angajați cât și de către angajatori deopotrivă a importanței unei conduite corespunzătoare.
- Utilizează pentru verificarea implementării acestei prevederi infrastructura deja existentă a ITM-urilor din țară.

Propunere de politică publică privind incriminarea corespunzătoare a unor fapte din sfera criminalității informatice care au produs consecințe deosebit de grave. Circumstanță agravantă

Formularea problemei:

În cazul în care statul român consideră oportună sancționarea mai aspră prin reținerea unor circumstanțe agravante asociate infracțiunilor informatice în ceea ce privește natura impactului asupra valorilor sociale protejate (relațiile sociale care iau naștere sau se manifestă ca rezultat al existenței și bunei funcționări a sistemelor informatice în diferite sectoare de activitate ori în plan economic și social), în ceea ce privește gravitatea pagubelor sau prejudiciilor ori a formelor de manifestare, este posibilă introducerea unei modificări la Codul Penal la sfârșitul Capitolului VI - Infracțiuni contra siguranței și integrității sistemelor și datelor informatice, din Titlul VII, mai înainte de „sancționarea tentativei", a unui articol nou care să incrimineze fapte care au produs efecte deosebit de grave, ca agravantă pentru toate infracțiunile informatice prevăzute la art. 360-365 și care poate fi un instrument oportun pus la dispoziția judecătorilor pentru a putea ține seama de aceasta la analizarea faptelor comise de autori și evaluarea tuturor circumstanțelor necesare pentru individualizarea pedepselor într-un mod corespunzător importanței valorilor sociale astfel protejate.

Scop:

Incriminarea corespunzătoare a unor fapte din domeniul criminalității informatice.

Obiective specifice:

Introducerea unei circumstanțe agravante la infracțiunile informatice din Codul Penal pentru faptele săvârșite împotriva sistemelor informatice și care au produs consecințe deosebit de grave.

Varianta propusă:

Amendarea Codului Penal prin introducerea, la sfârșitul Capitolului VI - Infracțiuni contra siguranței și integrității sistemelor și datelor informatice, din Titlul VII, mai înainte de „sancționarea tentativei", a unui articol nou cu următorul conținut:

Art. 3651 Fapte care au produs efecte deosebit de grave

Dacă faptele prevăzute în art.360-365 au produs consecințe deosebit de grave, au afectat semnificativ activitatea unei instituții din domeniile securității naționale, administrației publice, financiar-bancar, economic, energiei, transporturilor, telecomunicațiilor, sănătății sau mediului, ori au fost comise asupra datelor și sistemelor informatice care susțin infrastructuri critice naționale sau europene, așa cum sunt acestea definite de legislația în vigoare, limitele speciale ale pedepsei prevăzute de lege se majorează cu jumătate.

De asemeni, în situația în care autorul infracțiunilor informatice prevăzute la art. 360-365, în condițiile agravantei propuse mai sus, are acces la mecanismele de securitate ale sistemelor informatice (critice) afectate, în virtutea atribuțiilor sale de serviciu, ori are ca obligație asigurarea confidențialității și integrității datelor informatice sau buna funcționare a sistemelor informatice vizate de atacatori, **modificarea corespunzătoare a art. 66 Cod Penal în sensul introducerii unei pedepse complementare a interzicerii unor drepturi** - de exemplu dreptul persoanei de a mai ocupa o funcție similară ori de a mai răspunde de (a mai fi implicată în) administrarea de sisteme informatice, a mecanismelor de securitate asociate acestora, de a mai gestiona informații clasificate (potrivit legii) sau confidențiale ori date cu caracter personal - în general de a mai interacționa cu obiectele materiale ale valorilor sociale afectate prin acțiunea sau inacțiunea sa.

Propunere de politică publică privind incriminarea distinctă în Codul Penal a faptei de furt de identitate

Formularea problemei:

Din punct de vedere strict al faptelor comise, **nu există în acest moment o infracțiune care să poată fi reținută în sarcina unui atacator care obține neautorizat datele unei persoane**, iar activitatea acestuia pare că este de nepedepsit.

Scop:

Incriminarea corespunzătoare a unor fapte din domeniul criminalității informatice.

Obiective specifice:

Incriminarea faptei de furt de identitate comis prin utilizarea de sisteme informatice sau de mijloace electronice de comunicare.

Varianta propusă:

Amendarea Codului Penal prin introducerea unei noi infracțiuni care să vizeze furtul de identitate comis prin utilizarea de sisteme informatice sau de mijloace electronice de comunicare.

Textul incriminator propus:

Art. 000 ***Obținerea de date cu caracter personal, date de identificare, inclusiv date care permit utilizarea unui instrument de plata electronica sau orice alte date generate în cadrul activităților desfășurate de o persoană în plan social sau economico-financiar, fără acordul acesteia ori prin inducere in eroare, dacă fapta a fost săvârșită în sisteme informatice sau prin intermediul mijloacelor de comunicare la distanță, constituie infracțiune și se pedepsește cu închisoare de la x luni la y ani sau cu amendă.***

Propunere de politică publică privind clarificarea și armonizarea sensului unor noțiuni și expresii legate de domeniul informatic din Codul Penal și Codul de Procedură Penală

Formularea problemei:

Noul Cod Penal, deși preia integral infracțiunile din domeniul informatic care se regăseau anterior în Legea 161/2003, în schimb nu preia decât parțial și chiar incomplet definițiile privind înțelesul unor noțiuni specifice domeniului informatic.

Noul Cod de Procedură Penală, preia și el parțial din legea veche aceleași definiții incomplete, duplicând definițiile din Codul Penal.

Pe de altă parte, normele de aplicare ale noilor coduri nu abrogă articolul privind definițiile din legea 161/2003, astfel că în prezent avem următoarea situație de fapt:

- Art. 35 din legea 161/2003 este în vigoare
- Art. 181 Cod Penal definește incomplet doar doi dintre termenii care sunt definiți în Art 35 din Legea 161/2003
- Art. 138 Cod Procedură Penală definește și el, puțin diferit aceiași doi termeni care se regăsesc și în Codul Penal.

Scop:

Armonizarea legislației penale din domeniul criminalității informatice.

Obiective specifice:

- Corectarea definițiilor si sensului unor termeni și noțiuni specifice domeniului informatic

Varianta propusă:

Pentru armonizarea definițiilor și eliminarea duplicării definirii sensului noțiunilor, sunt necesare cumulativ următoarele amendamente și modificări:

- Amendarea Codului Penal actual în sensul preluării integrale a textului Art. 35 din Legea 161/2003 în cadrul textului Art. 181 Cod Penal.
- Abrogarea alineatelor 4 și 5 din Art. 138 Cod Procedură penală.
- Abrogarea Art. 35 din Legea 161/2003.

Titlul Proiectului: Sistemul Național de Combatere a Criminalității Informatice „Cyber Crime”

Proiect cofinanțat din Fondul Social European

Editorul Materialului: Centrul Național de Răspuns la Incidente de Securitate Cibernetică CERT-RO

Data Publicării: Mai 2014