R O M Â N I A

MINISTERUL AFACERILOR INTERNE
INSTITUŢIA PREFECTULUI – JUDEŢUL BUZĂU
COMISIA DE DIALOG SOCIAL

„MINUTĂ”
Ședința Comisiei Județene de Dialog Social Buzău
21.02.2024 ora 10:00

Comisia judeteană de dialog social, reorganizată prin Ordinul Prefectului Judetului Buzău nr. 34/18.01.2024, s-a întrunit astăzi 21.02.2024, la ședintă participând 13 dintre cei 21 de membri ai comisiei, temele abordate fiind*:*

1. *Evoluția fenomenului criminalității informatice, deficiențe și riscuri identificate.*
   Materialul este prezentat de către Agent șef de poliție ISPAS Ionuț-Corneliu.

Au fost prezenți 11 membrii din partea administrației, respectiv din Instituția Prefectului – Județul Buzău (dl. Prefect Daniel Marian Țiclea și dl. Subprefect Cristea Constantin), Consiliul Județean Buzău (dl. Marcel Lungu), Agenția Județeană pentru Plăți și Inspecție Socială Buzău (dna. Bănica Daniela), Agenția Județeană pentru Ocuparea Forței de Muncă Buzău (dl. Tociu Ionel), Direcția de Sănătate Publică Buzău (dl. Bolchi Lucian), Casa Județeană de Pensii Buzău (dl . Troncas Octavian), Inspectoratul de Politie Judetean Buzău (d-na Șocarici Mihaela și dl. Ispas Ionuț Corneliu), Direcția pentru Agricultura a județului Buzău (d-na Frățilă Maria), Inspectoratul Școlar Județean Buzau (d-na. Iordache Elena) și Inspectoratul Teritorial de Muncă Buzău (dl. Chitacu Bogdan).

Cefalan Laura Maria – secretar comisie.

Din partea Confederațiilor/Federațiilor sindicale și patronale au fost prezenți:

- Vasile Olteanu – BNS - Buzău
- Dobre Ion - Sindicatul Învățământului Preuniversitar ”Ion Neacșu” Buzău

Ședința a fost condusă de către dl. Prefect Daniel Marian Țiclea.

Conform reprezentantului I.P.J Buzău, prezent în cadrul ședinței, până anul 2019, competența materialului de instrumentare a infracțiunilor ce intră în sfera „infracțiunilor informatice” a aparținut

Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism, acestea fiind cercetate de către procurori cu sprijinul polițiștilor din cadrul Direcției de Combatere a Criminalității Organizate.

Începând cu data de 01.04.2019, dosarele penale având ca obiect infracțiunile prevăzute la art. 249 (frauda informatică), art. 250 (efectuarea de operațiuni financiare în mod fraudulos), art. 251 (acceptarea operațiunilor financiare efectuate în mod fraudulos), art.311 (falsificarea de titluri de credit sau instrumente de plată), art. 312 (falsificarea de timbre sau efecte poștale), art. 313 (punerea în circulație de valori falsificate), art. 325 (fals informatic) și 360 (accesul ilegal la un sistem informatic) din Codul penal, ce nu sunt săvârșite de săvârșite de grupuri infracționale organizate conform art. 367 (constituirea unui grup infracțional organizat) din Codul penal, au fost repartizate structurilor de investigații criminale ale Poliției Române, conform competențelor de supraveghere a urmăririi penale exercitate de unitățile de parchet.

Specific acestor infracțiuni este faptul că ele nu sunt localizate pe o anumită zonă, fiind efectuate în mediul online, autorii folosind metode de mascare a locației. O mare parte dintre aceste infracțiuni este săvârșită de către autori localizați într-o țară, iar victimele sunt din mai multe țări, nu doar din România.

Din punct de vedere statistic, în anul 2023 se observă o creștere cu aproximativ 30% față de anul 2022 a sesizărilor privind infracțiunile informatice, continuând trendul ascendent din anii anterior. Din totalul de dosare înregistrate circa 15% sunt fapte săvârșite prin modul de operare „investment scam”.

A. Investiții (Investment scam):

Folosindu-se de conturi furate de pe rețelele de socializare, conturi ce au aparținut unor persoane sau entități reale, autorii postează anunțuri cu privire la investiții în criptomonede sau acțiuni la diverse entități. Aceste anunțuri pot fi doar sub forma unor fotografii sau mesaje sau sub forma unor clipuri audio-video și se folosesc de imaginea unor persoane cunoscute în România, cum ar fi jurnaliști, oameni de afaceri, politicieni sau foști sportivi, toți având o anumită credibilitate în rândul cetățenilor români.

Ulterior accesării anunțurilor, persoanele vătămate sunt contactate telefonic sau prin aplicații de comunicare online de către autori, care se recomandă a fi brokeri sau analiști financiari, și li se solicită să trimită fotografii ale actelor de identitate și să instaleze diverse aplicații de control la distanță pe telefoanele mobile sau computere.

B. Phishing:

La bază, phishing-ul este o metodă frauduloasă prin care se încearcă obținerea unor date personale sau confidențiale precum detalii ale cărților de credit, parole sau cifre numerice unice. Hackerii primesc astfel acces la dispozitive sau conturi private fără ca utilizatorii să fie conștienți că le-au oferit acestora detaliile necesare. Prin phishing, victima accesează un link sau descarcă un fișier benevol, permițând astfel software-urilor să se infiltreze pe dispozitivul acestuia.

Phishing-ul se poate realiza prin două canale de comunicare:

- prin intermediul e-mail-ului - mesaj electronic trimis către un număr nedeterminat de destinatari (adresele lor fiind colectate prin diverse metode, prin intermediul Internetului), pretinzând a fi din partea unei surse legitime. Subiectul mesajului este conceput să atragă atenția (ex: “Mesaj important Actualizarea datelor personale”). De obicei, în conținutul mesajului de tip phishing sunt specificate măsuri punitive în cazul în care nu se va da curs solicitării (ex: “Imposibilitatea de a confirma detaliile contului online va duce la suspendarea definitivă a acestuia”). Se solicită

introducerea de date confidențiale folosind un link către un site indicat în textul mesajului (site fals, dar care reproduce foarte bine pagina originală)

Spear-phishing este un e mail sau o înșelătorie a comunicațiilor electronice orientate către o anumită persoană, organizație sau afacere atacurile de tip phishing nu sunt personalizate victimelor lor și, de obicei, sunt trimise la o masă de oameni în același timp.

- prin intermediul telefonului

Voice phishing(“vishing”) - Modalitatea prin care o persoană pretinde că sună din partea băncii și, invocând probleme tehnice (de ex în sistemul de plăți), solicită informații confidențiale cum sunt codul PIN, numărul contului, parola etc.

SMiShing - Actul de a folosi mesaje text de telefon mobil. Mesajele sunt similare celor primite prin e-mail și au același subiect, mai exact „Actualizarea datelor personale”, „Confirmarea detaliilor conturilor la aplicațiile bancare”.

Cel mai cunoscut exemplu pentru acest tip de infracțiune este „metoda OLX”, ce a avut o rată foarte mare de victimizare în perioada 2020-2022. Prin aceasta autorii își creau conturi pe platforma de vânzări on-line, contactau persoane care aveau anunțuri postate și le solicitau să continue conversația pe aplicațiile de comunicare („WhatsApp”), ocazie cu care induceau în eroare persoanele respective prin transmiterea de link-uri înșelătoare. Accesând riscurile respective, vânzătorilor li se solicita să introducă datele cardului bancar pentru a putea încasa contravaloarea produsului vândut, moment în care din contul persoanei erau transferate diverse sume de bani.

C. Citații:

Cetățenii pot primi pe e-mail, de la adrese aleatorii care par legitime, mesaje cu titulatura de ”CITAȚIE”. Acestea au atașate documente prin care li se comunică faptul că sunt vizați de acuzații pentru infracțiuni ce nu se regăsesc, ca și denumire, în legislația românească, respectiv „PORNOGRAFIE JUVENILĂ”, „PEDOFILIE”, EXHIBIȚIONISM”, CYBERPORNOGRAFIE”. Documentele respective poartă antetul și sunt emise în numele unor entități reale, cum ar fi INTERPOL, EUROPOL, DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ, entități ce au competență de a cerceta în mod direct infracțiuni, ci doar rol de suport pentru organele de cercetare penală. De asemenea pot fi emise în numele unor entități fictive, cu denumiri sugestive, tocmai pentru a crea o impresie de legalitate și o posibilă stare de „teamă” referitor la eventuale repercusiuni legale, cum ar fi POLIȚIA NAȚIONALĂ din cadrul MINISTERULUI APĂRĂRII, BRIGADA DE PROTECȚIE A MINORILOR.

D. Înșelăciuni romantice (Romance scam):

Autorii creează conturi pe rețelele de socializare, folosindu-se de fotografiile și numele unor persoane reale, în general cadre medicale sau ofițeri din cadrul forțelor armate străine, care activează în teatre de operațiuni și pretind că vor să se stabilească în România. Pentru aceasta, persoanele respective afirmă că au colete, trimise prin servicii poștale sau de curierat, care au fost oprite de autoritățile vamale și trebuie plătită o taxă vamală pentru a fi recepționate. Astfel persoanele înșelate sunt convinse să depună anumite sume de bani, cu scopul de a achita acea taxă vamala. După ce a fost trimisă o sumă de bani, autorii vor încerca să convingă persoana, folosind același pretext, să depună și mai mulți bani, până când victimele nu vor mai avea bani disponibili.

Au fost cazuri când victimele s-au împrumutat la rude, cunoscuți, bănci sau din alte surse pentru a trimite acele sume de bani.

E. Angajări:

Autorii creează pe rețelele de socializare anunțuri în numele unor entități reale prin care recrutează persoane pentru locuri de muncă „la distanță”, activitatea viitorilor „angajați” constând în vizualizarea unor reclame sau efectuarea unor „comenzi”/„sarcini”, urmând a fi plătiți pentru acestea. Este important de știut că, pentru a realiza activitățile repartizate, persoanele înșelate trebuie să depună sume de bani sau să accepte transferul prin conturile lor bancare a unor sume de bani.

F. Mistery box:

Autorii creează pe rețelele de socializare anunțuri în numele unor entități reale prin care promovează vânzarea de cutii misterioase, pline cu produse, ce par a veni de la comercianți mari, cunoscuți, sau bagaje pierdute de la companiile aeriene. Pentru a putea intra în posesia acestora, persoanelor vătămate li se va solicita să trimită anumite sume de bani.

G. Împrumuturi:

Autorii obțin, prin mijloace frauduloase, accesul la conturile de pe rețelele de socializare ale unor persoane. Ulterior aceștia contactează persoanele din cercul de prieteni al celor cărora le-au fost „furate” conturile și le solicită diverse sume de bani, sub formă de împrumut, motivând că trebuie să facă o plată și nu au suficienți bani sau că au cadrul bancar blocat și e o plată urgentă.

IV. DEFICIENȚE CONSTATATE:

Cadrul legislativ neadaptat la necesitățile și situația prezentă.

A. Dispozițiile privind „secretul bancar”, anumiți termeni din Codul de Procedură Penală.

B. Lipsa unui cadru legal care să oblige entitățile private străine, care desfășoară activități pe teritoriul României, să comunice date și informații către organele de poliție judiciară. Fiind diferențe legislative între țările în care acestea își au sediul și legislația națională, entitățile respectivă comunică date doar la solicitarea expresă a procurorului sau cu autorizare din partea unui judecător de drepturi și libertăți, deși legislația națională permite comunicarea datelor respective și către organele de poliție judiciară.

2. Lipsa unui canal comun de comunicare cu instituțiile financiar-bancare care oferă servicii pe teritoriul României și comunicarea deficitară a unor astfel de instituții (unele solicită documentele, fizic, prin poștă și răspunsul este transmis tot în format fizic, refuzul comunicării unor date fiind invocat secretul bancar inclusiv pentru imagini de la ATM-uri).

3. Lipsa unui mecanism de blocare/ștergere a unor postări, reclame, clipuri pe platformele de socializare sau de streaming video gratuite.

4. Deși Poliția Română și alte instituții ale statului (Ex. Directoratul Național de Securitate Cibernetică) și entitățile din domeniul financiar bancar au efectuat mai multe programe de prevenire, cu mesaje clare și exemple, acestea nu au fost receptate de către întreg publicul țintă, în special de către persoane în vârstă care nu au cunoștințe sau au cunoștințe minime în domeniul informaticii. De asemenea au fost mediatizate cazuri în care persoane au fost victimele unor astfel de infracțiuni, tocmai pentru a preveni alte preveni ca alte persoane să devină victime.

Ex.: Anumite entități din domeniul financiar-bancar au publicat în aplicațiile bancare mobile mesaje precum: „Nu dați curs reclamelor privind câștiguri din investiții! Puteți fi victimele unor fraude”, „Nu instalați aplicații de control la distanță!”

V. PROPUNERI PENTRU EFICIENTIZAREA ACTIVITĂȚII:

1. Modificarea unor acte normative pentru a adapta cadrul legal necesităților prezente și a facilita obținerea de date și informații.

A. Legea nr. 135 din 01.07.2010 privind Codul de Procedură Penal.

art. 153 - Obținerea de date privind situația financiară a unei persoane

(1) Procurorul poate solicita unei instituții de credit sau oricărei altei instituții care deține date privind situația financiară a unei persoane comunicarea datelor privind existența și conținutul conturilor unei persoane, în cazul în care există indicii temeinice cu privire la săvârșirea unei infracțiuni și există temeiuri pentru a se crede că datele solicitate constituie probe.

Având în vedere faptul că, pe această linie de muncă, majoritatea actelor de urmărire penală sunt întocmite de către organele de cercetare penală ale poliției judiciare, activitatea de cercetare penală ar fi ușurată semnificativ prin înlocuirea termenului „procurorul” cu termenul „organul de urmărire penale”.

B. Secretul bancar – Potrivit dispozițiilor art. 111 alin. (1) din O.U.G. nr. 99/2006, obiectul secretului bancar vizează „toate faptele, datele și informațiile referitoare la activitatea desfășurată, precum și orice fapt, dată sau informație referitoare la activitatea desfășurată, precum și orice fapt, dată sau informație, aflate la dispoziția instituției de credit care privesc persoana, proprietatea, activitatea, afacerea, relațiile personale sau de afaceri ale clienților – solduri, rulaje, operațiuni derulate –, la serviciile prestate sau la contractele încheiate cu clienții”. Client al unei bănci este orice persoană care beneficiază de serviciile acesteia, între el și bancă desfășurându-se o tranzacție, după cum este specificat în alin. (2), care este obiectul obligației de confidențialitate.

Astfel instituțiile financiare introduc sub „umbrela” secretului bancar și imaginile surprinse de camerele de supraveghere video montate în sediile acestora sau la ATM-uri, acestea considerând drept „client” persoana ce utilizează ATM-ul sau efectuează o operațiune, chiar dacă persoana respectivă nu are autorizarea titularului cardului, fiind autorul unei infracțiuni.

Având în vedere cele menționate supra, pentru a evita astfel de interpretări eronate există posibilitatea legislativă de a fi introdusă o prevedere în O.U.G. nr. 99/2006 prin care să se specifice în mod concret că imaginile surprinse de camerele de supraveghere video montate în sediile acestora sau la ATM-uri nu fac obiectul secretului bancar.

2. Crearea unui mecanism de cooperare/corespondare directă cu instituțiile financiare.

Ex.: Crearea unei platforme în care să fie interconectate instituțiile financiar-bancare și Poliția Română prin care solicitările să poată fi transmise direct, iar răspunsul să fie comunicat în același mod.

În prezent se utilizează adrese de e-mail ale instituțiilor și serviciile poștale sau de curierat, după caz.

3. Crearea unei structuri și a cadrului legislativ aferent în vederea blocării sau interzicerii unor elemente cu conținut malițios sau care sunt folosite în vederea săvârșirii de infracțiuni prin inducerea în eroare a persoanelor.

Reclame/clipuri audio-video cu privire la investiții în fonduri de investiții, acțiuni sau criptomonede ce promovează obținerea de câștiguri facile și substanțiale. Acestea sunt vizibile pe rețelele de socializare (Facebook, Instagram), platforme de streaming (Youtube, Tikok) și singura posibilitate de stopare a acestora, în prezent, este raportarea lor către platformele respective, măsură care, de cele mai multe ori, nu are niciun rezultat.

4. Achiziția de programe specializate în vederea efectuării de investigații și analize complexe, în special în sfera monedelor electronice.

Maltego, Chainalysis, Coinfirm, Coinpath, CipherTrace, Elliptic

Aceste soluții sunt greu de achiziționat deoarece sunt oferite de către entități private din afara României, iar pentru a se putea achiziționa prin licitație soluții oferite de aceste platforme ar fi necesar să aibă subsidiare sau contracte de distribuție cu entități de pe teritoriul României.

5. Organizarea de sesiuni de pregătire, altele decât cele organizate prin structurile de pregătire profesională al Poliției Române, care să fie susținute de experți din mediul privat, în vederea perfecționării polițiștilor din cadrul structurilor de combaterea criminalității informatice.

Prefect : Minuta urmează să fie înaintată la Ministerul Muncii și Solidarității Sociale- Direcția de Dialog Social și Ministerului Afacerilor Interne.

Vă multumesc pentru participare!

Copreședinții Comisiei Județene de Dialog Social Buzău

P R E F E C T, BUZĂU,

DANIEL - MARIAN ȚICLEA

PREȘEDINTE CONSILIUL JUDEȚEAN

PETRE EMANOIL - NEAGU