Către:

DELEANU ŞTEFAN LUCIAN

municipiul Cluj Napoca, str. Aurel Vlaicu nr. [redacted]

Nr. 364/19/P/2024 al Secţiei a III-a

în calitate de [Subiect]

ROMÂNIA
MINISTERUL PUBLIC
PARCHETUL DE PE LÂNGĂ ÎNALTA CURTE DE CASAŢIE ŞI JUSTIŢIE
DIRECŢIA DE INVESTIGARE A INFRACŢIUNILOR DE CRIMINALITATE ORGANIZATĂ ŞI TERORISM
STRUCTURA CENTRALĂ
SECŢIA DE COMBATERE A INFRACŢIUNILOR DE TERORISM ŞI A CRIMINALITĂŢII INFORMATICE

Bucureşti, Str. Sfânta Vineri, nr. 33, Sector 3, contact@diicot.ro
Telefon: 021.412.31.95, Fax: 021.319.39.30

Nr. 364/19/P/2024

Cod operator 16051
02/10/2025

Către,

DELEANU STEFAN LUCIAN
municipiul Cluj Napoca, [redacted] jud. Cluj

În temeiul disp. art. 316 alin. 1 Cod procedură penală, vă trimitem alăturat un exemplar al ordonanței nr. **364/19/P/2024** din data de **02/10/2025** a Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – Secția de Combatere a Infracțiunilor de Terorism și a Criminalității Informatice.

Totodată, vă comunicăm că, în temeiul disp. art. 339 alin. 4 Cod procedură penală, împotriva soluției de clasare puteți formula plângere în termen de 20 zile de la comunicare.

PROCUROR ŞEF SECŢIE, ***PROCUROR,***

ROMÂNIA
MINISTERUL PUBLIC
PARCHETUL DE PE LÂNGĂ ÎNALTA CURTE DE CASAŢIE ŞI JUSTIŢIE
DIRECŢIA DE INVESTIGARE A INFRACŢIUNILOR DE CRIMINALITATE ORGANIZATĂ ŞI TERORISM
STRUCTURA CENTRALĂ

Secţia de Combatere a Infracţiunilor de Terorism şi a Criminalităţii Informatice

Bucureşti, Str. Sfânta Vineri, nr. 33, Sector 3, cod operator 16051, contact@dilcot.ro,

Nr. 364/19/P/2024

02.10.2025

ORDONANŢĂ
de clasare

Procuror [redacted] din cadrul Direcției de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism – Secția de combatere a infracțiunilor de terorism și a criminalității informatice,

Examinând dosarul cu nr. de mai sus,

CONSTAT:

I. La data de 30.01.2024, pe rolul D.I.I.C.OT. – Structura Centrală a fost înregistrată sub nr. **364/19/P/2024**, plângerea penală formulată de **UNIUNEA NAŢIONALĂ A BAROURILOR DIN ROMÂNIA,** cu sediul în Bucureşti, Sector 5, Splaiul Independenței nr. 5, Palatul de Justiție, identificată prin C.I.F. RO 4315974, reprezentată legal prin Președinte Av. dr. Traian - Cornel BRICIU, e-mail: unbr@unbr.ro, împotriva:

- numitului **DELEANU STEFAN - LUCIAN,** născut la data de **19.10.2002,** în Municipiul **Suceava,** Județul **Suceava,** cu domiciliul în Județul Cluj, Municipiul Cluj - Napoca, [redacted] identificat prin C.N.P. [redacted] emisă la 16.12.2021 de SPCLEP Cluj - Napoca;
- **ENTRYRISE S.R.L.,** cu sediul social în Județul **Suceava,** Orașul **Gura Humorului,** Bulevardul Bucovina, Bloc D18, Scara A, Ap. 2, identificată prin J33/46/2021 și C.U.I./C.I.F. 43541700, având ca domeniu de activitate principal conform codificării (Ordin 337/2007) Rev. Caen (2) - Activități de realizare a soft-ului la comandă (software orientat client), reprezentată legal prin **asociat unic** și **administrator DELEANU ȘTEFAN - LUCIAN** (cu datele de identificare menționate

breșă de securitate ... sus), cu privire la care există o **suspiciune rezonabilă** în ceea ce privește ...ârșirea infracțiunilor de ***acces ilegal la un sistem informatic*** **(art. 360 Cod penal)** ***...transfer neautorizat de date informatice*** **(364 Cod penal)**

Prin ordonanța din data de 19.02.2024, s-a dispus *începerea urmăririi penale* în cauză, *"in rem"*, cu privire la săvârșirea infracțiunilor de accesul ilegal la un sistem informatic, prevăzută de art. 360 alin. 1, 2, 3 C.p. și transferul neautorizat de date informatice, prevăzută de art. 364 C.p.

În fapt, s-au arătat următoarele:

În data de **05 ianuarie 2024,** utilizând platforma informatică a domeniului **incorpo.ro** deținut de societatea **ENTRYRISE S.R.L.,** numitul **DELEANU ȘTEFAN – LUCIAN,** care în mediul virtual se prezintă ca fiind directorul societății, utilizând adresa de e-mail alexandra.ardelean@incorpo.ro (persoană virtuală creată prin utilizarea tehnologiei inteligenței artificiale - A.I.) transmite emailuri semnate de către numitul numitul **DELEANU STEFAN - LUCIAN** către un număr important de avocați, care se pretinde de către acesta că au fost obținute din baza de date administrată de **IFEP** împreună cu alte date referitoare la avocați (CNP, număr de telefon, număr de legitimație / card avocat CCBE) prin utilizarea unui *„endpoint accesibil fără parolă, și indexat de Google."*

Se susținea în e-mail că „acest endpoint a fost accesibil pentru aproximativ 2 ani". În cuprinsul e-mailului se arata totodată faptul că „a fost notificat IFEP în mod direct pe adresa de mail pentru a rectifica problema" și că „deși s-a rectificat în aceeași zi, avocații nu au fost notificați de existenta breșei".

Se recomandă în e-mail citirea „comunicatului de presă al Incorpo.ro referitor la breșa de securitate a IFEP".

Nu în ultimul rând, în partea finală a e-mailului se arată faptul că avocatul care dorește o probă cu privire la existența breșei este rugat să transmită prin e-mail la adresa office@incorpo.ro un document semnat electronic prin care să solicite expres și să furnizeze totodată societății ENTRYRISE S.R.L, care deține platforma domeniului incorpo.ro ,dreptul / acordul de procesare al datelor respective pentru a transmite avocatului totalitatea datelor obținute.

S-a arătat faptul că au fost avocați care au solicitat și au primit *CNP-ul* de la numitul DELEANU ȘTEFAN - LUCIAN.

În cuprinsul *„comunicatului de presă al Incorpo.ro referitor la breșa de securitate al IFEP"* publicat la data de 04 ianuarie 2024, actualizat în cursul zilei de 06 ianuarie 2024 și care poate fi accesat la următorul link: https://www.incorpo.ro/en-us/press/ifep-data-breach/?utm_nooverride=1&utm_source=smtp&utm_medium=newsman&utm_campaign=SMTP-20240105, se identifică un e-mail care se pretinde că s-ar fi transmis la data de 28 februarie 2023 către helpdesk@ifep.ro prin care ar fi fost sesizată pretinsa breșă de securitate din cadrul platformei IFEP.

Se pretinde prin „comunicatul de presă" faptul că „data la care a fost descoperită vulnerabilitatea coincide (dar nu are legătură) cu data propunerii de a construi o NOR pentru avocați", mai exact cu proiectul de lege privind serviciile profesionale efectuate de avocat în format electronic înregistrat la Senatul României sub nr. B47/2023 în data de 06.02.2023 și retras la data de 27.02.2023.

Prin același comunicat se arată totodată că există o breșă de securitate și în ceea ce privește platforma / baza de date a **CECCAR.**

În cuprinsul „comunicatului de presă al Incorpo.ro referitor la breșa de securitate al IFEP" publicat la data de **04 Ianuarie 2024** și actualizat în cursul zilei de **06 Ianuarie 2024** este inserată o *înregistrare audio - video* distribuită din platforma Youtube prin care numitul **DELEANU ȘTEFAN - LUCIAN** afirmă următoarele:

"Salut! Sunt **Ștefan Deleanu** și în acest videoclip voi discuta despre **breșa de securitate de la CECCAR și de la IFEP.** Modul în care le-am descoperit, n-am să explic de ce am făcut demersul de abia acum să notific public si să explic tot, tot ce s-a întâmplat în spate, tot background-ul, care a fost problema tehnică, riscurile, absolut tot, din perspectiva mea ca persoană care lucrează în IT și care are totuși tangențe cu Dreptul.

Însă, întâi de toate, vreau să tai niște percepții greșite pe care le-am văzut în mediul online. În primul și în primul rând, mail-ul respectiv nu a fost cu scop de marketing. Da, am publicat de pe o adresă de la Incorporo, pentru că deja avem infrastructura făcută. De aia am și trimis de pe Alexandra /Ardelean/, care e A.I.-ul nostru. Am trimis de pe acela, pentru că deja era tot sistemul setat, în afară de mici chestii care mi-a luat mult mai puțin să le fac decât dacă era să fac pe persoană fizică, aceleași demersuri.

Suplimentar, contabilii și avocații nu sunt ținta noastră. Noi suntem o platformă care țintim străini, nu avem absolut nicio legătură cu românii. Iar privitor la speța cu avocatura clandestină avem inclusiv o pagină unde discutăm de astă. Dar pe scurt, avem, generăm numai niște formulare, oamenii le semnează și noi le trimitem în mod automat. Inclusiv avem doctrină în străinătate care discută pe temă asta de completare de șabloane și achită de exercitarea fără drept a profesiei niște profesioniști care cu asta s-au ocupat.

Ok, întorcându-mă la problemă, eu am găsit de-a lungul activității mele mai multe breșe la diverse instituții publice, pentru că realitatea este că breșele astea sunt atât de frecvente și atât de multe, încât este extrem de dificil să le rezolvi. De multe ori am raportat niște probleme ca să nu fie rezolvate sau să fie rezolvate doar parțial, cu problemele încă persistente. În același timp, de foarte multe ori am raportat problemele astfel încât să mi se spună că se vor rezolva la următorul update, chiar dacă îmi ofereau acces asupra întregului spațiu web, spre exemplu. Și de aceea cred că am și ajuns la demersul ăsta în care am făcut totul public, pentru că mi se pare că dacă nu faci mizerie, din păcate, nu se rezolvă lucrurile. E trista realitate și modul în care funcționează societatea românească, în care dacă nu faci tam-tam și dramă, lucrurile nu se rezolvă.

Ca să discut punctual despre cum am făcut și cum am procedat, cât să fiu maxim de etic și să nu prejudiciez pe nimeni sau pe cât mai puțini și dacă am prejudiciat, voi plăti pentru prejudiciul pe care l-am cauzat și am să discut ulterior cam tot procesul și ce văd eu, cum văd eu, cum aș recomanda eu să procedeze și alte discuții pe/în temă.

Ideea e că în modul anterior, când eu raportam problemele, nu se prea rezolvau sau se rezolvau temporar și după, reapăreau. Însă în același timp, ca researcher în zona asta, în zona de Infosec, nu poți să te apuci și să spui pe internet din prima "vezi că aia are o breșă" când tu ești conștient că omul respectiv nu a rezolvat în totalitate breșa, nu a avut timp să analizeze, nu a avut timp să la demersurile interne cât să soluționeze și atuncea nu poți să o faci nici instant sau într- o lună sau în două, fără să îți asumi riscul că poate din vina ta, tu practic faci ceea ce ai încercat să previi și din contra, în loc să ascunzi măcar temporar sub preș, până rezolvi, groapa, tu practic arăți cu degetul spre groapă și îi faci pe oameni să sară în ea, lucru pe care tu nu vrei să-l faci. Evident, dacă scopul tău nu este să strici.

Problema punctuală e că pe IFEP, când căutam, discutam cu niște prieteni avocati care discutau pe proiectul de lege cu cloud-ul avocatilor, mi-au zis că e o problemă de lipsă de transparență cu IFEP. Și m-am pus să caut și eu, eram curios să văd ce e IFEP, cine îl

ANSPDCP-ul l-a prin
cât a trecut și acum
point-ul după ce i
e caz au zis că
asta o să se
, în sensul
te șapte
uranță
de
ă

ș.a.m.d. Și în căutările pe Google pe care le-am făcut am găsit și ASPX-ul respectiv îmi arăta toate endpoint-urile care erau, deci erau accesibile, publice și unul dintre endpoint-uri te punea să selectezi câți avocați să-ți arate, să arăți cu ce le începe numele, adică cu a, b, c sau chiar nu puneai nimic și să menționezi... mai aveau... da, numărul și o cheie care n-avea nicio relevanță. Și pe scurt, când apăsai pe enter și executai toată prostia ala, în mod automat, tie îți trimitea CNP-ul tuturor avocatilor în limita numărului ăla de căutări. Adică, dacă tu puneai să-ți apară 100, îți apărea **CNP-ul** la cei 100 cu prefixul respectiv. Și dacă puneai fără prefix și puneai 100.000 îți apăreau toți avocații, cu (toate CNP-urile, cu toate barourile la care lucrează. Pe un alt endpoint îți apăreau email-urile avocaților și pe acelea le-am și folosit ca să transmit ulterior. Au fost niște email-uri curate, anonimizate, pe care eu le-am folosit ulterior ca să trimit mail. Si într- adevăr, aici am încălcat GDPR-ul într-un mod evident si o și recunosc si-mi asum si amenzile, dacă sunt, pentru că, da, inclusiv prin faptul că am notificat niște persoane, eu am încălcat legea. Eu nu aveam niciun mod să soluționez asta sau să mă asigur că se soluționează fără să încalc legea, să comit un delict sau o faptă penală. Faptă penală nu am încălcat, că erau endpoint-uri publice si fix de aceea e si gravă situația, pentru că si la **CECCAR si la IFEP** erau niște endpoint-uri publice si pe care oricine le putea găsi pe Google. La CECCAR cred că endpoint-ul ăla era foarte frecventat, adică acolo-s aproape sigur că n-am fost singurul care a găsit problema. La IFEP, într-adevăr, era mai puțin frecventat link-ul și atunci e o mare probabilitate ca să fi fost printre singurii care au avut acces la respectivul endpoint și atunci poate e mai ok, dar concluzia pe care eu vreau să o trag e că faptul că am trimis mailurile respective în spam este pentru că altă soluție nu aveam ca să notific lumea. Am încercat să fac *ads* pe facebook și nu au văzut decât avocații din cercul meu restrâns, de persoanele pe care le cunosc de la Cluj sau colaboratori cu care am mai lucrat ș.a.m.d. și evident, scopul a fost să evidențiez problema la toată lumea, ca să știe lumea ce s-a întâmplat.

Acum, începând cu **IFEP**, pentru că a fost prima prima breșă care a apărut, deja am discutat, primul lucru pe care l-am făcut e să-i notific. Cred că în ziua viitoare sau chiar în aceeași zi le-am trimis un mail în care să-i notific la mail-ul care apărea pe site. Nu știam că e a UNBR si nu e OK să-i zici unui terț: /.../ e breșa. De aceea nici n-am notificat UNBR-ul si știu că purtam discuția cu niște avocati atunci, eu cum mă asigur să fac chestia asta fără să generez niște prejudicii, fără să pot să fiu acuzat ulterior că sunt complice la o faptă de acces neautorizat sau dracu știe! Pentru că se reține acces neautorizat și când plătești cu cardul și atunci îți pui problema dacă instituțiile publice sunt competente cât să analizeze o speță de genul și îmi era teamă. Acuma m-au luat dracii și am zis hai să pun fuck it și aia e, ce iese, o ieși!

Punctul 1. La **CECCAR** lucrurile erau și mai prost La CECCAR avea un endpoint unde căutai toți contabilii și puteai să-i cauți după nume, după email, după ș.a.m.d., număr de legitimație etc. Și it's ok, e necesar, ai nevoie de un astfel de program ca să poți să vezi dacă cineva e autorizat sau nu să facă contabilitate, expert sau autorizat. Și e normal ca CECCAR să aibă o astfel de listă, cum au și avocații și toată lumea. Problema e că acolo când căutai, în spate, endpoint-ul respectiv, când oricine, oricine făcea o căutare cu chestia aia pe care o folosea toată lumea care avea de căutat, îți apărea tot, de la CNP, la adresă, la data și locul nașterii, la sex, naționalitate, absolutamente tot era public, tot, tot, tot, tot tot! Și era un endpoint care nu numai că era public, ci nici măcar nu necesita interacțiune din partea utilizatorului sau unui actor malicios și literalmente toate persoanele care au intrat pe site-ul respectiv au avut acces la CNP-ul tău. El a fost stocat în memoria calculatorului lor.

Deci asta e problema punctuală și asta este problema pe care eu am încercat să evidențiez. Și la ei am procedat la fel, știind de situația care s-a întâmplat cu IFEP în mod anterior, când i-am notificat, am notificat DPO-ul, pentru că știam că ăla e răspunzător de partea legală, am notificat CECCAR-ul pe mail-ul direct și am notificat și ANSPDCP-ul, pe care

I-am pus în BCC ca să nu vadă băieții că eu am trimis la ANSPDCP. ANSPDCP-ul l-a prim... I-a lăsat la ei la timp, a trecut cred că 90 de zile sau nu știu din septembrie câți a trecut și acum primesc răspunsul de la ANSPDCP că ei nu au văzut, că au verificat endpoint-ul după ce l... rezolvaseră, rezolvaseră în vreo cred că 3 zile după ce am raportat și în orice caz au zis că nu sunt probe. Le-am trimis toată baza de date, pentru că eram aproape sigur că asta o să se întâmple, pentru că asta este demersul pe care l-am văzut la toate instituțiile publice, în sensul în care se mușamalizează și s-a mușamalizat peste tot, peste tot și am raportat peste șapte astfel de breșe. Unele breșe care... dar aia s-a gestionat. OK, care era de risc de siguranță națională, deci putea să genereze panică în rândul populației generale. Ăla e nivelul de probleme care sunt și ăsta e nivelul de soluții pe care tu trebuie să le faci ca tu să poți să notifici și să iei măsuri, pentru că în mod contrar nu le pasă. ... În fine, am văzut chestia asta, le-am trimis la ANSPDCP tot exportul, că de altundeva n-aveam de unde să-l am, e evident, adică erau datele lor profesionale toate, plus CNP, toate prostiile alea, erau singuri care aveau acces. Într-adevăr, am comis și eu un delict și-mi asum și asta este, acces neautorizat nu putea să fie că era un endpoint public, toată lumea avea acces, singura diferență între mine și ei, că eu am salvat intenționat să-l țin ca probă. Și asta a fost povestea. Și acuma ANSPDCP-ul are informațiile acolo.

Văzând modul în care au abordat CECCAR problema, am zis fuck it, hai să facem asta și cu avocații. Mi-au zis toți avocații "nu fă", "nu fă", toți pe care-i cunosc, pentru că, da, deschizi cutia pandorei și e un risc pe care tu, odată ce ți-l asumi, e posibil să ieși fără libertate. Suntem în România, suntem într-o țară unde te poți aștepta la absolut orice. Și atuncea... Știi, pe mine nu mă avantajează cu absolut nimic că am făcut reclamă la o breșă și mi-am făcut și mie reclamă de om bun de mers la pușcărie. Nu, nu mă, nu mă avantajează cu absolut nimic. Ba, da. Oleacă de brand awareness pentru mine ca persoană și cam atât. Deci nu pot să neg că sunt și niște avantaje aici, dar exclusiv atât. Și oricum toate demersurile astea au început prin plângeri, prin lucruri pe care nu le-am făcut publice, 90% din ceea ce fac nu fac public. În fine, asta le-am făcut publice și am decis să fac mail-ul ăla, să fac cele două publicate și să le notific pe toată lumea de toate problemele care apar. Și acuma văd că de-abia acuma să iau măsuri. De abia acuma lumea s-a sesizat. ... E tristă realitate și modul în care funcționează societatea, din păcate, în România. Nu suntem o societate care să conștientizeze riscurile și să le prevină, ci una care le atacă odată ce există. Și în momentul în care tu dezvălui lucrurile astea, este atacat cel care o dezvăluie și este atacat cel care a fost vinovat. Și după aia, e un joc de resurse. În fine, noi am făcut raportul ăsta, cei de la CECCAR au dat un raport că ei nu au fost notificați și nu știau, după ce ANSPDCP-ul are mail-ul unde vede că doar au fost și chiar au și trimis un răspuns, evident, eu am făcut copy la toate mail-urile, la toate notificările, bază de date să nu zică că nu a fost breșa. După aia au zis că de fapt eu le-am furat bază de date că... deci eu n-am avut acces, dar eu le-am furat baza de date! La care eu nu aveam acces. Și nici măcar nu-i furt ăla că ar fi acces neautorizat, dar acces neautorizat cum? că era un endpoint public și oricine căuta prin tabloul ăla nu prea să vadă decât dacă făcea endpoint-ul ăla. Adică atâta vreme dacă voiai să vezi că cineva e contabil și noi căutam contabil că aveam nevoie să luăm la Incorporo să putem să recomandăm la clienți niște contabili și căutam pe acolo oameni. Dacă căutai, pac, ai și comis infracțiunea! **Evident că dacă ar fi să o considerăm pe aia acces neautorizat, atuncea îs mai multi infractori decât putem să numărăm.** Ar trebui DIICOT-ul să-și facă un corp special pentru toată infracțiunea asta, dacă aia e infracțiune. Evident, e o absurditate și nu este. În fine, ideea e că am făcut demersul, am notificat pe toată lumea și acuma merg pe transparență, n-am, eu nu cred că am ce să ascund și atuncea dau totul pe față, vine organul de urmărire penală, mă saltă, îmi sparge ușa, no problem, să vadă, să verifice, să analizeze, să răsanalizeze, că nu, nu văd o problemă și aia e, adică, na, la final eu îs destul de safe. Într-adevăr, există riscul să... că na, e vorba aceea,

vine polițistul după tine și te tot urmărește, găsește ceva, dar sperăm că lumea e de bună credință și acea... Doamne ajută! No, bun.

În esență, am făcut notificare la ambii. Mulți s-au temut de faptul că e fals, e o țeapă, o înșelăciune, nimeni nu a avut acces și aici am să discut o leacă de tema asta. Dacă ești avocat și vrei să îți furnizez datele care au apărut în breșă, eu pot să fac asta dacă îmi trimiți un email sau ceva într-un mod în care pot să-ți verific cel puțin identitatea, adică fie să mă contactezi de pe email-ul pe care te-am notificat eu, pentru că ăla era din baza de date a IFEP. Plus să-mi zici numele tău întreg și dacă-mi oferi cele două, eu pot să-ți arăt tot ce era în baza de date. Dar cumva trebuie să văd că tu ești cel care deții, ca să nu dau CNP-uri la oameni pe net, că nu ăsta-i scopul. Deci de aici și o leacă este mai scurting stilul meu, de aia am fost vag, de aia n-am dat toate informațiile pe față, pentru că e foarte dificil să demonstrez că există breșa fără să fii cel care practic o generează și atunci am încercat cumva să fiu sensibil și pe zona de CECCAR și pe zona de avocați. La CECCAR am făcut o chestie mai riscantă, am făcut o chestie în care-ti arăta datele anonimizate si îti păstram numai primul și ultimul caracter sau primele două și ultimele caractere, ca să vadă lumea că bă, de unde dracu are datele astea, că n-avea de unde. Și am băgat ăsta pe site, deși e o breșă clară a regulamentului GDPR și iar îmi asum aici o amendă pe persoană fizică că no, dar asta este, îmi asum amenda și să fac un grup found me dacă-mi iau amendă de la cei care au fost ajutați de faptul că cineva le-a notificat faptul că există probleme. Deci mie mi se pare că, într-adevăr, da, am comis un delict cu speranța să previnâ unul mai mare care chiar poate să fie și infracțiune dacă se apucă unul să șteargă niște mail-uri știind că el trebuia în mod normal să notifice. În fine.

Cam asta e povestea. Eu în continuare stau extrem de transparent și dacă aveți întrebări, dacă vreți să discutați cu mine, să vă explic punctual cum a funcționat problema, eu sunt accesibil și oricând pot să răspund la întrebări, numa timp, că primesc foarte multe mesaje în momentul curent și atuncea le iau pe rând. Asta e tot. Mulțumesc foarte mult de timp și zi frumoasă și somn ușor și scuze pentru mesajul târziu, că presupun că n-a prins cel mai bine. Chiar, chiar îmi pare rău. Na, intenția a fost să comunic. Mulțumesc foarte mult. Zi frumoasă și spor la treabă!"

S-a arătat în continuare faptul că, la solicitarea **U.N.B.R.** de a se oferi clarificări cu privire la situația reclamată, societatea **INTRA CONNECT S.R.L.** a comunicat în scris faptul că:

- „prin raportare la elementele existente în spațiul public, cu referire specifică la endpoint- ul menționat, respectiv https://www.ifep.ro/Ws/InternalWebServices.asmx, putem concluziona că acest endpoint nu prezintă, din punctul nostru de vedere, riscuri de securitate."

- „în endpoint-ul menționat nu există niciun indiciu că ar exista posibilitatea unei breșe de securitate, însă portalul IFEP este actualizat permanent, iar din 28 februarie 2023, data la care se face referire că s-a identificat incidentul și până la data curentă, portalul IFEP a suferit numeroase modificări."

***

II. La data de 06.02.2024, pe rolul D.I.I.C.OT. – Structura Centrală a fost înregistrată sub nr. **610/19/P/2024** și plângerea penală formulată de **CORPUL EXPERȚILOR CONTABILI ȘI CONTABILILOR AUTORIZAȚI DIN ROMÂNIA (CECCAR)**, persoana juridica romana de utilitate publica si autonoma, cu sediul in București, str. Intrarea Pielari nr. 1, sector 4, reprezentata prin Președintele Consiliului Superior, doamna Elena- Ecaterina CHIVU, împotriva aceluiași **DELEANU STEFAN – LUCIAN** și totodată societății la care acesta are calitatea de asociat unic și

administrator, respectiv societatea **ENTRYRISE S.R.L.**, cu privire la care există o suspiciune rezonabilă în ceea ce privește săvârșirea infracțiunilor de *acces ilegal la un sistem informatic* (art. 360 Cod penal) și *transfer neautorizat de date informatice* (364 Cod penal).

Prin ordonanța din data de 20.02.2024, s-a dispus *începerea urmăririi penale* în cauză, "in rem", cu privire la săvârșirea infracțiunilor de accesul ilegal la un sistem informatic, prevăzută de art. 360 alin. 1, 2, 3 C.p. și transferul neautorizat de date informatice, prevăzută de art. 364 C.p.

În fapt, s-au invocat aceleași aspecte faptice, referitoare la identificarea vulnerabilități tehnice de către numitul DELEANU STEFAN LUCIAN, respectiv:

La data de 06.01.2024, numitul DELEANU Stefan-Lucian a transmis un email (pe care il semnează cu numele si mentionarea calitatii sale de director al societății ENTRYRISE S.R.L.), de la adresa office@incorporo.ro la adresa dpo@ceccar.ro destinata responsabilului cu protecția datelor din cadrul CECCAR, avand ca atașament o parte din baza de date cu caracter personal si confidential privind membrii CECCAR (nume si prenume, cetățenie, CNP, data si locul nașterii, adresa si numărul de telefon, adresa de e-mail, număr de autorizație profesionala si alte detalii profesionale).

De asemenea, sus numitul a utilizat adresele de e-mail apartinand membrilor CECCAR, conținute de baza de date a CECCAR, si a transmis o expunere sub titlu de notificare privind o breșa de securitate a sistemului informatic care i-ar fi permis accesul la date personale (informatii pentru care accesul publicului ar fi fost restricționat de Corpul profesional prin masuri tehnice specifice).

Corespondenta a fost transmisa de pe o adresa de email prin platforma incorporo.ro, iar in conținut s-au utilizat link-uri către site-ul companiei ENTRYRISE S.R.L, care prezentau oferte comerciale ale companiei.

Se arată că în același sens, al faptelor savarsite prin afectarea securității bazei de date personale stocata in platforma *https://raport.ceccar.ro* găzduită pe serverul de date al *CECCAR* și utilizarea abuziva de date cu caracter confidential, numitul DELEANU Stefan-Lucian a procedat la un autodenunț, sub forma de înregistrare audio-video, făcut public de acesta pe pagina de internet *incorpo.ro*, devoalând acțiunile sale, în mod explicit, la care a aplicat cunoștințe, peste medie, de inginerie web. Pretextele pe care le expune pentru fapta sa, precum dorința sa de a mobiliza instituțiile profesionale si autoritățile statutului în scopul înlăturării unor vulnerabilități ale sistemelor informatice/bazelor de date, nu au susținere legala si nu îl absolvă de răspunderea prevăzută de lege.

S-a menționat ca, anterior, respectiv la data de 07.09.2023, numitul DELEANU Stefan-Lucian a transmis prin email (de la aceeași adresa office@incorporo.ro către subscrisul Corp profesional (la adresele contact@ceccar.ro si dpo@ceccar.ro), un mesaj in sensul ca ar exista o « *potențiala breșa de securitate* » a unui « *număr semnificativ de date personale* » operate de CECCAR in evidentele sale informatizate, sus numitul oferindu-se disponibil pentru *«consultanta si asistenta pentru solutionarea problemelor»*.

Fata de aceste împrejurări s-au efectuat verificări de către DPO-ul CECCAR (respectiv DAIKOKUTEN S.R.L, in calitatea sa de specialist responsabil cu protecția datelor cu caracter personal procesate de operatorul CECCAR), potrivit Raportului din

...ata de 07.09.2023 intocmit pentru situația data, concluzionând la acel moment ca *„Nu există certitudinea că au fost extrase /copiate date cu caracter personal din baza de date»*.

In autodenuntul făcut public, DELEANU Stefan-Lucian afirma ca la momentul septembrie 2023 a notificat si Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, autoritate care, in urma verificărilor celor sutinute de sus-numitul, a contrazis afirmațiile acestuia, in sensul ca o simpla cautare publica pe site-ul CECCAR, la rubrica destinata tabloului membrilor-profesionisti contabili, nu acceseaza si nu face disponibile datele confidențiale pretinse.

Se mai arată în cuprinsul sesizării, faptul că sunt relevante articolele publicate pe pagina de facebook a numitului DELEANU Stefan - Lucian si pe site-ul www.incorporo.ro, prin care prezintă critici si acțiuni întreprinse la adresa CECCAR si UNBR, nemulțumiri subiective si teorii in consecința, generate de imposibilitatea ca sus-numitul si societatea sa ENTRYRISE S.R.L. (incorporo.ro), la care este asociat unic si administrator, nu pot desfasura activitatile pe care si le doresc pentru ca activitatile vizate intra sub autorizările legale profesionale date de legiuitor in sarcina CECCAR si UNBR.

In aceleași articole anterior descrise, sunt menționate si breșele de securitate pretinse la aceste corpuri profesionale, atat la CECCAR cat si la UNBR, precum si demersuri făcute referitor la acestea (*„...fara expunere publica, nu se rezolva nimic, si UNBR si CECCAR de exemplu au negat breșele de securitate.”*).

Întrucât între cele două cauze există o strânsă legătură, ambele sesizări fiind îndeptate împotriva acelorași persoane fizice/juridice, prin ordonanța din data de 20.02.2024, s-a dispus reunirea dosarului pena cu nr. 610/19/P/2024 al DIICOT – S.C. la dosarul penal cu nr. 364/19/P/2024 al DIICOT – S.C.

În cauză, s-a procedat la analizarea datelor existente la dosar, a datelor existente online și a tuturor datelor și înscrisurilor solicitate și furnizate organului de urmărire penală, de catre U.N.B.R., C.E.C.C.A.R. si A.N.S.P.D.C.P., fiind reținute în continuare următoarele (proces-verbal de analiză date/înscrisuri):

A.

Publicare bresa de securitate UNBR – 28 Februarie 2023

În urma verificării datelor postate de catre numitul Stefan-Lucian Deleanu referitor la bresa de securitate UNBR, la URL https://www.incorpo.ro/en-us/press/ifep-data-breach/?utm%20nooverride=1&utm_source=smtp&utm_medium=newsman&utm_campaign=SMTP-20240105#steps-taken, s-a stabilit ca există o postare si un document pdf ce face referire la o posibila bresa de securitate in ceea ce priveste date cu caracter persoanal ce a avut loc anterior datei de 05.01.2024 pe infrastructura aferenta portalului IFEP "https://www.incorpo.ro/content/files/2024/01/Probleme-de-securitate--Portalul-IFEP.pdf"

Probleme de securitate - Portalul IFEP

"Stefan Deleanu" <office@entryrise.com> February 28, 2023 at 1:46 PM

To: helpdesk@ifep.ro

Buna ziua,

Va contactez pentru a raporta urmatoarele probleme de securitate informatica, pe care le-am identificat in timpul utilizarii platformei IFEP.

Am identificat urmatoarele probleme:

- **Bresa date cu caracter personal (Risc Ridicat):** API-ul accesibil AICI este public, si poate fi utilizat desi informatiile furnizate prin intermediul acestui API sunt informatii cu caracter personal. Spre exemplu, prin interogarea endpoint-ului "GetLawyersFull", un actor malicios poate obtine informatii referitoare la numele, prenumele, baroul unde sunt inregistrati, precum si CNP-ul persoanelor inscrise in tabloul furnizat de IFEP, care ar simplifica o potentiala uzurpare a calitatii de avocat de catre un astfel de actor.
- **Lista unui sistem de autentificare sigur (Risc Ridicat):** S-a apreciat ca utilizarea CNP-ului ca sistem unic de securizarea a platformei nu este o solutie ideala, fiind informatii care pot fi usor identificate sau deduse dupa un minim de analiza in informatiile disponibile publice. CNP-ul este format, in mare parte, din date asociate direct datei nasterii, genului, judetul nasterii, 3 numere care reprezinta seria nasterii (de la 001 la 999), precum si un cod de paritate calculat in baza celorlalte. Un atacator ar putea afla CNP-ul doar printr-un simplu bruteforce, cu 999 incercari, ulterior validand CNP-ul prin autentificarea reusita.
- **Potential risc de furt conturi (Risc Mediu):** In contextul in care un numar de telefon (neasociat contului) si CNP-ul profesionistilor sunt unicele date necesare pentru resetarea parolei, un atacator care cunoaste CNP-ul victimei ar putea sa se utilizeze de acesta, si un numar virtual, pentru a obtine acces in contul victimei.
- **Potential risc de deanonimizare a voturilor prin platforma (Risc Redus):** In contextul problemelor sus mentionate, un atacator care dispune de CNP-ul persoanei (de pe care se poate obtine, in mod direct, codul CCBE), ar putea da bruteforce pe hash pentru a afla variabilele necunoscute (CodSecuritate, Pozitii Votate). In lipsa unui seed unic, atacul devine, de asemenea, exponential mai usor.

Recomandari de natura tehnica:

- Abordarea unei scheme de incredere "Zero Trust". Furnizarea minimului necesar de incredere utilizatorilor, pana la demonstrarea autorizatiei de accesare a datelor (spre exemplu, prin autentificarea intr-un cont cu privilegii).
- Modificarea schemei de autentificare cat aceasta sa includa informatii care nu pot fi deduse in baza informatiilor publice (Spre exemplu, prin utilizarea unui email si cod utilizator, si validarea manuala a cererilor de schimbare a parolei in baza unui document semnat cu semnatura electronica calificata).
- Restrictionarea accesului la API-uri interne, in contextul in care accesul nu este necesar pentru functionarea platformei.

Pentru orice detaliu de natura tehnica, sau orice alta intrebare, va stau la dispozitie pe email, sau telefonic.

Multumesc Mult,
Deleanu Stefan-Lucian

Stefan-Lucian Deleanu
Director / ENTRYRISE S.R.L

Articolul face referire la url : InternalWebServices Web Service (ifep.ro) care ar fi fost anterior acelei date și susceptibil de-a furniza date cu carcater personal din tabloul avocatilor din Romania, prin introducerea unor criterii simple de cautare. https://www.ifep.ro/Ws/InternalWebServices.asmx?op=GetPersonal

URL ul furnizeaza o optiune de a trimite o cerere SOAP către un server web prin intermediul metodei POST. URL- ul exista si in prezent dar completarea de criterii nu returneaza nici un rezultat.

In acest sens, se concluzioneaza, ca daca pana la acea data a existat acea posibilitate care nu poate fi exclusa prin datele ce se detin la dosar, in prezent nu mai există aceasta posibilitate.

Documentatia si datele furnizate de catre U.N.B.R.:

1.

17042024_Raport_Evaluare_Raspuns_Incident_Analiza_Digital_Forensics_IFEP_v1

cuprinde analiza detaliată a logurilor sistemului pentru IFEP și din care se concluziile investigației efectuate în cauză, astfel cum sunt redate în cele ce

Trasee de Audit: În cadrul investigației de digital forensics realizate pentru Uniunea Națională a Barourilor din România (UNBR), s-au identificat câteva limitări semnificative în ceea ce privește configurarea și gestionarea logurilor sistemului IT. Aceste deficiențe au avut un impact direct asupra capacității noastre de a reconstitui evenimentele și de a evalua amploarea unui posibil incident de securitate."
Din cauza configurațiilor inadecvate ale logurilor și a schimbării versiunii platformei între momentul presupusei breșe și timpul investigației, este dificil de determinat cu precizie dacă un acces neautorizat a avut loc. În plus, nu a fost păstrată o imagine a platformei de la momentul incidentului, ceea ce îngreunează reconstituirea exactă a stării de securitate. Cu toate acestea, analiza actuală nu a identificat dovezi directe ale unei breșe.

Acest raport prezintă rezultatele analizei detaliate a logurilor sistemului pentru IFEP (fișiere de jurnalizare – 11584 fișiere au fost analizate), cu accent pe identificarea oricăror scurgeri de date potențiale din portalul UNBR. Pe baza analizei amănunțite a logurilor disponibile la momentul evaluării și a configurației sistemului de logare existentă, raportul constată că nu există dovezi digitale care să indice scurgeri de date din portal.

Analiza a relevat că sistemul de logare a fost configurat să înregistreze doar activități din IP-uri interne (din rețeaua 192.168.1.0/24) și de pe endpoint-uri de test specifice (railways.tests.ifep.ro). Această configurație limitează semnificativ capacitatea de a obține o perspectivă completă asupra tuturor solicitărilor și interacțiunilor cu portalul, excluzând în mod efectiv orice acces extern direct din analiză.

Logurile furnizate, care acoperă perioada presupusului incident, nu oferă informații suficiente despre evenimentele de autentificare sau modificările de configurare ale sistemului. Această lipsă de detalii ne împiedică să urmărim eficient cine s-a conectat la sistem, când exact s-au realizat aceste conexiuni și dacă au existat încercări nereușite de autentificare - un posibil indicator al unor tentative de acces neautorizat.
În plus, absența informațiilor specific
legate de modificările de configurare obstrucționează capacitatea noastră de a identifica și evalua acțiunile interne ce ar putea influența negativ integritatea și securitatea sistemului.
Analiza a relevat că, deși a
administratorul platformei, Intra Connect SRL, a
reacționat la notificarea incidentului, lipsa unui protocol standardizat de răspuns la incidente a limitat capacitatea de a gestiona eficient situația.
Administratorul a efectuat revizuiri ale configurațiilor de securitate și a verificat jurnalele disponibile, însă aceste acțiuni au fost constrânse de lipsa solutiilor specifice de monitorizare pentru intruziuni si setările inițiale de baza ale sistemului de logare.

Concluzii

Raportul concluzionează că, în prezent, platforma este securizată conform rezultatelor recente ale testelor de penetrare, care indică faptul că o breșă similară cu cea presupusă nu ar putea avea loc în configurația actuală a platformei. Aceasta nu exclude posibilitatea unui incident anterior, ci subliniază limitările tehnice ale echipamentelor și procedurilor de logare folosite în momentul presupusului incident. "

2. 17042024_Raport_Teste_de_Penetrare_pentru_Platforma_IFEP_v1.0-1.pdf

" În cadrul testelor de penetrare efectuate recent pe platforma IFEP, a fost identificată o singură vulnerabilitate de nivel scăzut: detaliile excesive în mesajele de eroare. Este important de înțeles că, în funcționarea oricărei aplicații digitale, întâlnim momente neprevăzute care pot genera erori. Răspunsurile sistemului la aceste situații pot varia de la simpla notificare a utilizatorului că a survenit o eroare, până la furnizarea unor informații suplimentare despre natura problemei.
Cu toate că scopul acestor mesaje este de a ajuta în identificarea și rezolvarea erorilor, unele dintre ele pot oferi detalii neintenționate despre structura internă a sistemului (de exemplu, versiunea serverului sau detalii tehnice). Această practică poate oferi un avantaj neașteptat persoanelor rău-intenționate, permițându-le să găsească puncte slabe specifice pe care să le exploateze în atacuri mai sofisticate.
Astfel de mesaje "verbale" pot dezvălui informații despre componentele software folosite, ceea ce ar putea indica metode de atac prin Injecție SQL (SQLi) sau Cross-Site Scripting (XSS), sau chiar pot facilita identificarea numelor de utilizator prin enumerare.

Rezultate Teste de Penetrare:

- *Vulnerabilități de Nivel Scăzut: Prezența unor vulnerabilități minore, cum ar fi informațiile excesive în mesajele de eroare, care ar putea fi exploatate de atacatori pentru a obține detalii despre infrastructura tehnică.*
- *Recomandarea de revizuire a politicilor de gestionare a erorilor pentru a minimiza riscurile.*
-
- *Stabilitatea Sistemului: În general, platforma a arătat o stabilitate impresionantă, neexpunând vulnerabilități critice sau semnificative în timpul testelor de penetrare.*
-

***Concluzii:** Evaluarea a evidențiat că, deși platforma IFEP este bine protejată și robustă în fața amenințărilor cibernetice, există nevoia de îmbunătățire continuă a gestionării erorilor pentru a crește securitatea. Este esențială implementarea unor măsuri suplimentare de securitate pentru a contracara posibilele breșe care pot fi exploatate prin vulnerabilitățile minore identificate."*

3. Raspuns INTRA CONNECT SRL (administratorul platformei)- solicitare DIICOT.docx

„

- *Metode de extragere a datelor: datele sunt extrase prin următoarele metode:*
  - *interogări directe ale bazei de date cu rezultat afișat în formularele web;*
  - *interogări web service interne prin afișare rezultat în diverse obiecte existente în aplicații (gen obiecte de tip select);*
  - *execute metode de export date în excel, prin intermediul unor evenimente integrate în aplicație;*
  - *interogări API externe pe bază de API Key și furnizare date în format JSON.*
- *Interfețe publice de acces:*
  - *https://www.ifep.ro/Justice/Lawyers/LawyersPanel.aspx - Interogare directă a bazei de date;*
  - *https://cautavocat.ro/ - extragere periodică a datelor prin API, populare bază de date aferentă website-ului și afișare informații în paginile web;*
  - *Aplicația de mobil a UNBR – interogare API pentru validarea calității de avocat a utilizatorului.*
- *Securitate și acces:*
  - *accesul la API se realizează pe bază de API key, fiind implementate și mecanisme de filtrare la nivel de IP*
  - *accesul la metodele existente în web service-ul intern sunt securizate prin API Key, filtrare la nivel de IP și autentificare (pot fi consumate doar de utilizatorii autentificați).*
- *Interfețe de test și mentenanță: testarea aplicației se realizează prin publicarea unei versiuni beta pe serverul de producție, la adresa https://www-staging.ifep.ro*

„

Așadar, din analiza conținutului acestor date si documente, a rezultat ca în urma auditului local de Securitate, nu s-a putut stabili cu certitudine dacă anterior datei de 05.01.2024 a existat o bresa de securitate care sa vulnerabilizeze datele cu caracter personal existente pe platforma IFEP.

Totusi acest lucru este în contradictoriu cu cele menționate de catre UNBR prin reprezentanti in sesizarile catre DIICOT si ANSPDCP. De asemenea acest fapt este in contradictoriu și cu elementele tehnice prezentate în datele publicate despre bresa de securitate și in avertizările transmise de numitul Stefan Deleanu.

Imposibilitatea auditului local de securitate, de stabilire retroactivă a existenței sau nu a respectivei breșe de securitate sesizată și notificată în cauză, s-a datorat

(astfel cum de altfel se și menționează în raportul mai sus amintit), faptului că, inadecvata configurație ale logurilor și a schimbării versiunii platformei între momentul presupusei breșe și momentulinvestigației, a făcut dificilă determinarea cu precizie dacă un acces neautorizat a avut loc. În plus, nu a fost păstrată o imagine a platformei de la momentul incidentului, ceea ce a îngreunat reconstituirea exactă a stării de securitate.

De asemenea, a rezultat că logurile furnizate, care acoperă perioada presupusului incident, nu au oferit informații suficiente despre evenimentele de autentificare sau modificările de configurare ale sistemului. Această lipsă de detalii au împiedicat să se urmărească în mod eficient cine s-a conectat la sistem, când exact s-au realizat aceste conexiuni și dacă au existat încercări nereușite de autentificare - un posibil indicator al unor tentative de acces neautorizat.

In acest sens, se concluzionează că dacă la momentul sesizarii bresei ar fi putut exista posibilitatea afisarii in modul de dezvoltator a unor date suplimentare, date transmise de catre API, la pachet cu datele afisate, la momentul actual infrastructura nu mai furnizează astfel de date.

În fapt Stefan Deleanu indica faptul ca bresa de securitate a existat în site-ul UNBR incepand cu aprilie 2021 si a durat pana la mijlocul anului 2023.

Rezultatele analizei facute de catre acesta:
Risk assessment and CVSS details - 5.5/10
The vulnerability was assessed based on criticality, impact, and exploitability using the CVSS scoring metric, with an estimated CVSS Score of:

- CVSS Base Score: 7.5/10
- Impact Subscore: 3.6/10
- Exploitability Subscore: 3.9/10
- CVSS Temporal Score: 7.2/10
- CVSS Environmental Score: 5.5/10
- Modified Impact Subscore: 1.8/10
- Overall CVSS Score: 5.5/10

În prezent, aceste date nu mai pot fi verificate faptic pe site-ul UNBR si pe infrastructura respectiva deoarece API-ul si site-ul au fost modificate de catre proprietar.

B. Bresa de securitate publicată în 7 Septembrie 2023 (CECCAR)

Din datele on-line si de la dosar se constata ca anterior datei de 07.09.2023 ar fi existat o bresa de securitate care a vulnerabilizat date cu caracter personal pe platformaCECCAR.

Numitul Stefan-Lucian Deleanu indica vulnerabilitatea în postarea aflată la URL: https://base-docs.incorpo.ro/press/ceccar-data-breach/

In acelasi URL se afla un raspuns al ANSPDCP cu numarul 16863 din 07.09.2023 care explica faptul ca nu au fost identificate la acel moment date cu caracter personal in afisarea site-ului CECCAR in afara celor de contact

In urma verificarii datelor și informatiilor din raspunsul inițial al CECCAR au fost observate o serie de omisiuni si inadvertente si au fost în continuare solicitate clarificari.

Din analiza raspunsurilor comunicate de către CECCAR s-au desprins urmatoarele concluzii :

- Sistemul a avut o perioada în care a transmis prin API către browserele utilizatorilor mai multe date decat sunt transmise in prezent in baza unui Search Query (interogare), existand posibilitatea reala ca un utilizator legitim sa poata obtine mai multe date despre persoane decat numele, prenumele, numarul de telefon si orasul. Astfel a existat operioada in care cererea API returna mai multe informatii și chiar daca acestea nu erau afisate direct in fereastra browserului ele erau primite public de persoana care cauta pe site in cadrul raspusului API.
  In concret o persoana sau un program automat putea obtine in mod public si neîmpiedicat de masuri de securitate date persoanale suplimentare despre persoanele afisate pe site-ul CECCAR.
- In luna august 2023 a existat cel putin o situatie documentata si cunoscuta de catre CECCAR cu privire la faptul ca sistemele transmiteau si expuneau mai multe date decat era necesar catre utilizatori in baza interogarilor efectuate pe site. Acest fapt, printre altele, este congruent cu situatia raportata de numitul Deleanu Stefan.
  În acest sens:
- (Raspuns firma IT CECCAR : „În raspunsul returnat de functie, nu se intorceau doar datele strict necesare ci se intorcea un set exhaustiv de informatii legate de ID ul interogat, acestea fiind chiar cele din CSV-ul transmis de persoana acuzata")
- (Raspuns firma IT CECCAR: *"datele transmise ca exemplu si primite de daniela.popa22@gmail.com sunt in formatul livrat de API* si nu au fost niciodata afisate ca atare de UI; acestea nu au fost niciodata afisate ca atare in productie sau pe orice platforma expusa la internet , ele putand fi vizualizate exclusiv prin accesarea modului Developer a unui browser")

Desi API-ul (Application Programming Interface) furniza informatiile extinse despre persoanele de pe site, firma IT si CECCAR considera totuși ca acestea nu erau publice.

Această susținere nu se poate fi primită în mod just și de o manieră logică, în condițiile în care orice fel de dată transmisă în baza unui "query" (interogare), fara autentificare, de catre un sistem informatic, este o *dată publică*, putând fi accesată de către orice persoana cu acces la internet sau sistem automat de colecare a datelor.

A rezultat totodată, că în urma verificarii in prezent a platformei CECCAR si a raspunsului oferit de acestea, utilizand optiunea de dezvoltator din browser nu s-a constatat aparitia in zona de raspuns a altor date decat cele de contact ale expertilor, la un moment dat, problema fiind între timp remediată.

În urma verificarii, s-a stabilit ca în secțiunea response, nu apar date cu caracter personal.

Aşadar, şi în acest caz, se reţine faptul că, la momentul sesizării breşei ar putut exista posibilitatea afisarii in modul de dezvoltator a unor date suplimentare, însă la momentul actual infrastructura nu mai furnizeaza astfel de date.

Rezultă astfel date şi indicii temeinice, că date suplimentare, nenecesare au fost expuse de sistem, public, către internet, datorită configurării defectuase a API, indicii ce susţin de altfel varianta prezentată de către Deleanu Stefan.

Din analiza răspunsului Autoritatăţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal (A.N.S.P.D.C.P.), au rezultat urmatoarele:

- sesizările formulate de Uniunea Naţională a Barourilor din România (UNBR) înregistrate la ANSPDCP sub nr. 422/10.01.2024, 448/10.01.2024 şi 694/15.01.2024;
- sesizarea formulată de Corpul Experţilor Contabili şi Contabililor Autorizaţi din România (CECCAR) înregistrată la ANSPDCP sub nr. 1402/25.01.2024.

Cu privire la această situaţie, ANSPDCP a demarat investigaţii la operatorii UNBR (pe data de 11.01.2024) şi CECCAR (pe data de 10.01.2024), ca urmare a sesizărilor formulate anterior de numitul Deleanu Ştefan-Lucian (în data de 07.09.2023, 03.01.2024, respectiv 08.01.2024) şi a formularului de notificare a încălcării securităţii datelor cu caracter personal transmis de CECCAR în data de 08.01.2024.

Din analiza tuturor răspunsurilor şi datelor comunicate în prezenta cauzp, considerăm că nu au rezultat date concrete de natură să contureze în mod legitim faptul că, la baza incidentelor de securitate soldate cu expunerea publică a datelor cu caracter persoanal, a stat o acţiune intruzivă, ilicită, efectuată fără drept asupra bazelor de date, acţiune care să aibe ca scop obţinerea de date confidenţiale aparţinând celor două corpuri profesionale.

A rezultat faptul că numitul Deleanu Stefan a avertizat asupra breşelor de securitate în data de 07.09.2023, CECCAR şi respectiv în data de 28.02.2023, UNBR.

Cu toate acestea, se constată că a existat un spatiu mare de timp între semnalarea problemelor tehnice şi raportările facute de CECCAR, respectiv UNBR la ANSPDCP, neexistând un raţionament sau motiv logic sau legal pentru aceast ecart.

În consecinţă, pe baza datelor existente si obtinute, a analizelor efectuate, se poate concluziona faptul ca au existat probleme certe în construcţia , managerierea si programarea infrastructurii celor 2 site-uri (CECCAR si UNRR), situaţie care a condus la posibilitatea obiectiva de accesare publică a unor date personale de către utilizatori legitimi ai spaţiului de internet. Printre aceşti utilizatori a figurat si numitul Deleanu Stefan, care în fapt a şi sesizat breşele de securitate la instituţiile reclamante, demers finalizat cu formularea unor plângeri penale împotriva acestuia.

Fiind audiat în cauză, numitul DELEANU STEFAN – LUCIAN a confirmat încă o dată aspectele de fapt care au stat la baza constatării şi notificării celor două breşe şi incidente de securitate care au putut conduce la posibilitatea accesării publice în reţeaua de internet şi luării la cunoştinţă într-un mod neîngrădit a datelor cu caracter personal.

În esenţă, a acesta a declarat că firma sa, Entryrise SRL are o componenta care furnizeaza sabloane pentru infiintarea si desfasurarea activitatii de societati comerciale, sens în care, cauta permanet colaboratori pe acest segment.

In continuare, a procedat la crearea unui proces automat (program informatic) de obtinere a datelor publice de pe site-ul CECCAR referitoare la contabili afisati, pentru a l se crea o lista de potentiali colaboratori pe care urma sa il contacteze.

Programul informatic creat este legitim si a fost creat de el, avand o arhitectura simpla care descarca si salva informatiile afisate pe site-ul CECCAR la acea data, urmand ca ulterior sa le organizeze in alt format. Acest tip de program este folosit in mod curent pe Internetul public pentru diverse activitati de acumulare si structurare de date inclusiv pentru marketing sau crearea de arhive, inclusiv de catre Google.

Dupa ce a rulat programul, datele publice au fost descarcate peste noapte, a doua zi s-a uitat pe ele si a remarcat faptul ca exista o discrepanta evidenta intre ce se afisa in fereastra de browser si datele furnizate efectiv catre browser (prin API) de catre serverele CECCAR.

In fapt , datele furnizate catre Browser de catre serverele CECCAR contineau pe langa cele afisate si date care nu ar fi trebuit sa fie transmise de catre server, respectiv CNP, domiciliu, seria si numarul cartii de identitate.

Vazand acest lucru si avand expertiza in domeniu, a concluzionat rapid ca exista o problema de securitate cu site-ul si serverul respectiv, deoarece aceste date nu ar fi trebuit sa fie transmise de catre server.

De asemenea a mentionat faptul ca datele transmise de server in format extins care contineau si date cu caracter personal erau transmise automat catre orice sistem informatic (utilizator al site-ului) care efectua o cautare simpla vizuala pe site, cu particularitatea ca datele personale extinse erau transmise de catre server catre browserul utilizatorului (oricare ar fi el), dar nu erau afisate pe ecran, ele fiind primite de browserul utilizatorului si salvate in fisierele temporare ale browserului respectiv si prezente in memoria RAM.

Acest aspect este prevalent in toate comunicatiile dintre un browser si un server web, in sensul ca de cele mai multe ori serverul web trimite mult mai multe date si informatii decat percepe un utilizator pe ecran. Particularitatea aici este ca in mod concret serverul web CECCAR ar fi trebuit sa fie setat sa nu trimita datele cu caracter personal extins pe care CECCAR le detinea pe arhitectura sa, pentru ca in caz contrar oricine le putea descarca involuntar prin simpla accesare a site-ului si vizualizare a unui contabil sau a unei liste de contabili.

Nu își mai aduce acum aminte exact data, dar la scurt timp dupa ce a sesizat problema, a notificat CECCAR, prin email si concomitent in aceeasi comunicare a sesizat problema la ANSPDCP (in BCC – BCC insemana ca mesajul email a fost transmis in acelasi timp la CECCAR si la ANSPDCP, dar CECCAR nu putea sa vada ca ANSPDCP a primit acelasi email de notificare).

CECCAR i-a raspuns pe email dar nu își mai aduc amintește ce i-au scris, insa acel mesaj este pus pe site-ul unde a notificat public existenta incidentului.

ANSPDCP i-a raspuns la mesajul email si i-a spus ca initial nu poate confirma existenta vulnerabilitatii. A presupus astfel ca ei au cerut date de la CECCAR si acestia din urma au infirmat existenta unei astfel de vulnerabilitati.

Ulterior a transmis catre ANSPDCP copia datelor publice pe care le-a descarcat spunandu-le ca CECCAR a indus in eroare ANSPDCP cu privire la existenta acelei vulnerabilitati si brese. ANSPDCP i-a confirmat ca a primit datele si i-a solicitat sa trimită orice alta informatie despre situatia descrisa. Le-a trimis in plus corespondenta

cu DPO-ul CECCAR (DPO - persoana responsabila cu protectia datelor cu caracter personal). Ulterior nu își mai amintește daca ANSPDCP a mai facut comunicari directe catre el pe aceasta problema, avand multe mesaje pe diverse probleme cu acestia.

La scurt timp a sesizat ca CECCAR a remediat vulnerabilitatea, dar nu a informat contabilii, asa cum prevede legea. Discutand cu prieteni contabili pe Messenger, acestia i-au comunicat ca nu au fost informatii despre existenta bresei.

Astfel, a decis sa transmită mesaje de avertizare către contabili afișați pe site, prin email. Mesajul continea date despre cand a fost gasita vulnerabilitatea, tipul de datele personale expuse (nu datele propriu zise), informatii cu privire la riscurile la care au fost expusi si datele de contact ANSPDCP.

Dupa ceva timp am vazut pe grupurile de Facebook ale contabililor o serie de postari ale acestora in care spuneau ca au primit mesaje si email-uri de la CECCAR in care se mentiona ca nu a existat nici o vulnerabilitate si că îi vor face plângere pentru furt de date.

A mentionat faptul ca plangerea penala facuta de CECCAR s-a formulat doar dupa ce el a informat contabilii despre vulnerabilitate. Personal consideră astfel că plangerea penala a fost facuta ca o masura punitiva si de răzbunare impotriva sa, pe motiv ca a facut publica existenta vulnerabilitatii si a informat ANSPDCP si toti contabili despre asta.

Fata de cele mentionate mai sus, a precizat ca nu a desfasurat nici o activitate infractionala de tip Hacking , datele pe care le-a obtinut fiind accesibile in mod public si nerestrictionat, putând fi accesate si descărcate automat de orice utilizator al site-ului CECCAR, el fiind doar cel care a remarcat vulnerabilitatea si a facut notificare despre ea. De altfel, a stres aceste date descărcate imediat dupa ce a notificat ANSPDCP.

Referitor la situația si vulnerabilitatea descoperită pe site-ul UNBR, a mentionat ca atunci cand se căutau pe Google toate paginile web de pe site-ul IFEP.ro, exista o pagina web publica care descria modul in care se pot accesa mai multe API-uri publice (API ul este o interfata de programare automata specifica serverelor web care, printre alte functii, in cazul de fata, permite vizualizarea tuturor avocatilor, baroul de provenienta si adresa email).

Primul API permitea accesarea numelui, baroului și adresei de email, iar al doilea API public permitea accesarea numelui, CNP-ului si a identificatorului unic din sistem din baza de date (un număr crescător atribuit de sistem pentru fiecare dintre avocati).

A intrat din Browser pe ele, apasand click pe butonul „get lawyers", a introdus caracterul „spatiu" si intr-o căsuța de filtrare a scris sa imi afiseze „100000" si a apasat butonul „cautare".

In acel moment, site-ul i-a transmis urmatoarele date aferente avocatilor: identificatorului unic din sistem din baza de date, adresa de email , nume/prenume, baroul de provenienta.

Tot din browser amdat click pe butonul „get full lawyers", a urmat aceleasi etape si i-a afisat pe ecran: nume/prenume, identificatorului unic din sistem din baza de date, baroul de provenienta si CNP-ul.

In urmatoarea zi, a notificat administratorul platformei IFEP.ro, respectiv firma INTRACONECT (despre care a aflat ulterior, deoarece in prima instanta a initiat

contactul prin helpdesk@ifep.ro) si le-a spus ca API-urile publice par a transmite date care nu ar fi trebuit transmise (ex. CNP) . A asteptat un raspuns, dar nu l-a mai primit.

Ulterior a transmis avocatilor prin email un mesaj in care le descriam problema pe care eu a descoperit-o, riscurile asociate si sa îl contacteze pentru mai multe detalii.

Unii dintre ei l-au contactat solicitandu-i informatii suplimentare despre bresa de securitate, el comunicându-le aceste informatii. Le-a spus ca problema a fost remediată intre timp, dar ca o perioada de timp aceste tipuri de date au fost expuse public.

Vulnerabilitatea si descrierea situației a fost trimisa de catre el si catre ANSPDCP in fereastra de timp dintre momentul remedierii vulnerabilității si informarea pe care a trimis-o eu catre avocati.

Plangerea facuta de catre UNBR a venit dupa ce a informat avocatii, la aproximativ o luna de zile dupa informarea avocatilor, nu își mai aduce aminte exact și la un an distanta de momentul în care eu a sesizat vulnerabilitatea la helpdesk@ifep.ro,

El nu a stiut mult timp despre faptul ca UNBR a facut plangere penala impotriva sa, afland cu ocazia acestei audieri. Consideră ca aceasta plangere penala are de asemenea un caracter de represalii impotriva sa, fiind facută târziu si fiind nefondata.

La un moment dat pe Facebook, a fost contactat de catre o persoana care s-a prezentat ca fiind în conducerea UNBR și care l-a intrebat daca situatia descrisa este adevarată , iar el a confirmat.

A mai mentionat faptul ca pe site-ul pe care erau furnizate functiile API se facea mentiunea expresa despre cum se pot accesa acestea, descrierea serviciului, modul de accesare a acestuia si ghidul de accesare a datelor.

Având în vedere toate aspectele de fapt rezultate din probele administrate în cauză, apreciem că nu poate fi angajată răspunderea penală a numitului DELEANU STEFAN – LUCIAN, totodată reprezentant al societății Entyrise SRL, sub aspectul săvârșirii celor două infracțiuni reclamate în cauză de către reprezentanții UNBR și CECAR, respectiv infracțiunile de acces ilegal la un sistem informatic și transfer neautorizat de date informatice, fapte de natură informatică și îndreptate împotriva siguranței și integrității sistemelor și datelor informatice.

Sub aceste aspecte, apreciem că faptele sesizate nu se pot imputa persoanelor reclamate, nici din punct de vedere obiectiv și nici subiectiv. În cauză, nu sunt îndeplinite și întrunite elementele constitutive sub aspectul tipicității obiective ale unor asemenea fapte penale și deopotrivă, nu se poate considera că acțiunile, întreprinse în cauză de numitul DELEANU STEFAN – LUCIAN (pe fondul existenței prealabile a celor două breșe de securitate ce au condus din neglijență/neatenție la expunerea către public a unor date cu caracter personal) de accesare, interogare, căutare și descărcare de date din sistemele informatice accesibile publicului, au fost îndeplinite cu rea-credință. Nu se poate astfel considera că în cauză, acesta a acționat în forma de vinovăție prevăzută de lege, respectiv cu intenția calificată de a obține, fără drept, date confidențiale cu caracter personal (exp. CNP) aparținând avocaților/contabililor, prin operațiuni intruzive și neautorizate și care să fi avut drept țintă sistemele informatice care stocau astfel de date private și neexpuse în mod public.

Pentru aceste motive,

În temeiul dispoziţiilor art. 315 al. 1 lit. b C.p.p. rap. la art. 16 lit. b C.p.p. art. 3 alin.(3) Cod proc. pen., art. 316 alin. (1) din C. proc. pen.,

DISPUN :

1. **Clasarea** cauzei sub aspectul săvârşirii infracţiunilor de accesul ilegal la un sistem informatic, prevăzute de art. 360 alin. 1, 2, 3 C.p. și transferul neautorizat de date informatice, prevăzute de art. 364 C.p., fapte sesizate împotriva numitului DELEANU STEFAN – LUCIAN și S.C.ENTRYRISE S.R.L. (reprezentată legal prin asociat unic și administrator DELEANU ȘTEFAN – LUCIAN) de către UNIUNEA NAȚIONALĂ A BAROURILOR DIN ROMÂNIA (U.N.B.R) și CORPUL EXPERȚILOR CONTABILI ȘI CONTABILILOR AUTORIZAȚI DIN ROMÂNIA (CECCAR).
2. Cheltuielile judiciare rămân în sarcina statului.
3. Soluția se comunică.

PROCUROR

[redacted]