BRANDEFENSE COUNTRY REPORT · ROMANIA 2026

Brandefense: Raport privind amenințările cibernetice din România 2026

Oferte de acces, recuperarea serviciilor și limitele dovezilor despre spionaj

Odin by Brandefense

Perioada analizată: 1 ianuarie–22 noiembrie 2026, după data publicării postării

Versiunea 1.0 · Ediție publică de cercetare · TLP:CLEAR · 8–22 noiembrie 2026

250
domenii candidate în douăsprezece grupe sectoriale

14
dosare detaliate de anunțuri, cu limite distincte ale dovezilor

12
etichete de grupări ransomware în populația înregistrărilor românești

18
acțiuni cu responsabili și dovezi observabile

CUPRINS

Cuprins

Translated with AI

Această ediție a fost tradusă cu AI din originalul în limba engleză. În cazul unor diferențe, prevalează ediția în engleză.

01	Rezumat pentru conducere	05
	Harta raportului	09
02	Contextul digital și de securitate al României	10
03	Expunerea națională: domenii de organizații selectate	14
04	Ce arată dovezile din mediul clandestin	22
05	Incidente oficiale și decizii sectoriale	47
06	Hactivism, DDoS și activitate recentă	81
07	Grupări, persoane și relații susținute de dovezi	91
08	Economia fraudei	103
09	Sectorul bancar și serviciile financiare	109
10	Reglementare și răspuns național	113
11	Perspective	118
12	Plan de acțiune	122
A	Anexa A. Sferă și limitele dovezilor	128
B	Anexa B. Registrul dovezilor	131
C	Anexa C. Surse	133
D	Anexa D. Glosar	138
E	Anexa E. Alte constatări oficiale și context de campanie	140
	Despre raport	142

Consiliu și conducere	01 05 11 12
CISO	03 04 05 07
SOC și infrastructură	03 04 06 07
Fraudă și relații cu clienții	08 09 12
Juridic și comunicare	05 06 10

Despre această ediție

Tradus cu AI din ediția în limba engleză. În cazul unor diferențe, prevalează ediția în engleză. Cercetarea și redactarea au beneficiat de asistență AI. Declarațiile surselor, afirmațiile infractorilor, observațiile și evaluările analitice sunt prezentate distinct.

Dovezile din România cer control practic asupra accesului administrativ, documentelor sensibile, furnizorilor și recuperării, cu o decizie separată pentru fiecare afirmație neverificată.

773.764

postări etichetate România; nu atacuri

20

înregistrări ransomware pentru România; afirmații infracționale

250

domenii candidate selectate în douăsprezece sectoare

50/100 (B)

valoarea națională Atlas pentru portofoliul selectat

Cuprins și trasee de lectură

Raportul leagă deciziile conducerii de dovezile păstrate. Fiecare capitol începe cu o întrebare și se încheie cu trei concluzii. Anexele precizează limitele surselor, populațiilor și termenilor.

Capitol	Întrebare	Cititor principal
1 Rezumat	Ce decizii au prioritate?	Conducere
2 Context	Ce dependențe din România influențează răspunsul?	CISO
3 Expunerea organizațiilor	Ce observații pot fi susținute pentru domeniile selectate?	Infrastructură
4 Activitate clandestină	Ce s-a oferit și ce rămâne neverificat?	Informații despre amenințări
5 Cazuri sectoriale	Ce stabilesc comunicările oficiale?	Responsabili de servicii
6 DDoS și activitate recentă	Ce s-a schimbat între 8–22 noiembrie?	Operațiuni
7 Grupări și persoane	Ce atribuiri și relații sunt susținute?	Informații despre amenințări
8 Fraudă	Cum devin informațiile o instrucțiune neautorizată?	Prevenirea fraudei și relații cu clienții
9 Sector bancar	Ce controale cer implicarea securității, trezoreriei și echipelor pentru clienți?	Servicii financiare
10 Reglementare	Ce termene de raportare și excluderi se aplică?	Juridic și conformitate
11 Perspective	Ce ar modifica evaluarea?	Conducere
12 Plan de acțiune	Cine acționează în 30, 60 și 90 de zile?	Toți responsabilii
Anexele A–E	Care sunt limitele dovezilor, sursele și definițiile?	Toți cititorii

Traseu pentru conducere: capitolele 1, 3, 5 și 10–12. **Traseu operațional:** capitolele 4, 6–7 și 12. **Traseu pentru identitate și fraudă:** capitolele 3, 8–9 și 12.

Observație înseamnă că deținem postarea sau măsurătoarea. **Afirmație** înseamnă că autorul susține un rezultat. **Relatare oficială** înseamnă o constatare comunicată de o autoritate sau organizație, în limitele precizate. **Deducția analitică** leagă dovezile de o decizie.

Existența unui anunț nu autentifică materialul oferit. Confirmarea oficială a unui incident poate lăsa neclarificate accesul inițial, copierea, populația și autorul.

CAPITOLUL 01

Rezumat pentru conducere

01

ÎNTREBAREA ACESTUI CAPITOL

Ce decizii rezultă direct din dovezile păstrate și comunicările publice verificate din România?

4

decizii pentru conducere, cu responsabili și dovezi de finalizare

Patru decizii pentru conducere 07

Anul în cifre 07

CAPITOLUL 01

Rezumat pentru conducere

PE SCURT

Amenințările vizibile din România combină oferte de date și acces, înregistrări de șantaj și relatări oficiale despre servicii perturbate. Noiembrie a adus relatări noi despre spionaj mai vechi, oferte recente de acces și constatări ale autorității de protecție a datelor. Ransompedia deține 20 de înregistrări pentru România în interval. Niciuna dintre aceste populații nu reprezintă totalul național de incidente. Verificați conturile privilegiate, protejați documentele și accesul furnizorilor și demonstrați recuperarea fluxurilor esențiale.

Raportul combină postări Brandefense Blackhole, înregistrări Ransompedia, observații Atlas privind expunerea și controalele pasive ale domeniilor selectate și relatări publice verificate la sursă. Fiecare populație are o unitate, o dată și o limită distinctă. Domeniile selectate nu estimează prevalența națională. [S1][S2][S3]

Intervalul solicitat se încheie la 22 noiembrie. Dovezile reflectă ce era disponibil în timpul cercetării din acea zi. Nu reprezintă un inventar complet până la sfârșitul zilei. Perioada finală, 8–22 noiembrie, apare separat în capitolul 6.

1. Ofertele de acces cer dovezi despre conturi. Materialul de pe forumuri include acces la portaluri prezentate ca guvernamentale, oferte de acces la distanță și o ofertă de administrator pentru o platformă comercială, din noiembrie. Acestea demonstrează publicarea anunțurilor, fără să confirme acces funcțional, tranzacții sau o anumită cale de intrare. Eticheta vânzătorului trebuie să declanșeze verificarea de către responsabilul contului. [S1]

2. Documentele creează risc de fraudă înainte de clarificarea originii. Ofertele descriu evidențe despre clienți, salarizare în educație, contracte turistice și documente ale unor servicii juridice private. Numărul pretins de documente nu este numărul persoanelor. Nici informațiile autentice nu ar demonstra că fiecare contraparte numită a suferit o intruziune. [S1]

3. Vizibilitatea ransomware susține pregătirea recuperării. Ransompedia înregistrează 20 de mențiuni pentru România sub douăsprezece etichete de grupări, față de 17 în întregul an 2025. Qilin apare în 7 dintre înregistrările din intervalul curent. Comparația dintre un an parțial și un an complet nu este o rată de creștere pentru perioade egale. Înregistrarea rămâne o afirmație infracțională. [S3]

Țările de comparație au fost selectate ca exemple doar pentru a oferi context; alegerea lor nu implică un clasament sau o evaluare politică.

4. Relatările recente despre spionaj au o cronologie mai veche. Cercetarea ESET din 10 noiembrie descrie un caz Exchange guvernamental început în decembrie 2025, cu activitate în ianuarie 2026. SRI afirmă la 11 noiembrie că a identificat atacul în decembrie, l-a oprit și nu a identificat exfiltrări de date sensibile. Păstrați limitele ambelor surse, fără să rezolvați diferențele în lipsa unor dovezi suplimentare. [S6][S7][S8]

5. Constatările privind datele extind agenda controalelor. Comunicările oficiale descriu slăbiciuni ale accesului la distanță, acces neautorizat al angajaților și erori de prelucrare, alături de atacuri cibernetice. Programul defensiv are nevoie de guvernanța accesului, administrare sigură și controale de proces. Numărarea exclusivă a atacurilor externe ar omite aceste lecții. [S33][S37][S39][S40]

6. Ofertele curente de autentificare cer verificare. 79 dintre cele 250 de domenii selectate aveau date de autentificare oferite la vânzare. Valoarea națională Atlas este 50/100 (B). Cel puțin 356.395 de asocieri de dispozitive și 1.355.738 de evidențe de autentificare susțin verificări separate, fără a stabili intruziuni curente. [S2]

Patru decizii pentru conducere

1. **Atribuiți verificarea conturilor unei echipe responsabile.** Confirmați că alertele despre date de autentificare și acces ajung la echipa de identitate. Corelați fiecare semnal cu conturi active, privilegii și sesiuni. Escaladați utilizarea neautorizată demonstrată; închideți materialele istorice sau fără corespondent cu un motiv consemnat.
1. **Protejați documentele și la furnizori.** Identificați cine poate exporta informații juridice, despre clienți, angajați și plăți. Testați alertarea furnizorilor, păstrarea dovezilor și revocarea accesului. Analizați dacă un document legitim ar putea susține o instrucțiune frauduloasă chiar când sursa inițială este incertă.
1. **Demonstrați recuperarea independentă.** Restabiliți un flux esențial folosind copii protejate și date de autentificare separate pentru recuperare. Cereți acceptarea rezultatului de către responsabilul serviciului. Includeți comunicarea cu clienții și dependențele de furnizori în exercițiu.
1. **Folosiți o singură cronologie factuală pentru raportare și comunicare.** Consemnați separat detectarea, luarea la cunoștință, impactul asupra serviciilor și constatările ulterioare. Furnizați aceleași fapte echipelor juridice, de protecție a datelor și de comunicare. Distingeți publicarea recentă de atacul recent.

Anul în cifre

Cifrele de mai jos descriu populații distincte. Nu trebuie adunate.

773.764

Postări etichetate România în intervalul solicitat, după data postării [S1]

CE NU REPREZINTĂ

Atacuri, persoane afectate sau incidente unice

41.379

Postări distincte în arhiva păstrată pentru raport [S1]

CE NU REPREZINTĂ

Întregul mediu clandestin românesc sau un eșantion reprezentativ

256

Postări de forum etichetate România, păstrate [S1]

CE NU REPREZINTĂ

256 de incidente sau oferte verificate independent

14

Postări din 8–22 noiembrie în acel set [S1]

CE NU REPREZINTĂ

Paisprezece atacuri noi

20

Înregistrări ransomware pentru România în interval [S3]

CE NU REPREZINTĂ

Criptare, furt de date sau persoane juridice distincte, confirmate

17

Înregistrări pentru România în întregul an 2025, în aceeași situație de date [S3]

CE NU REPREZINTĂ

Referință pentru o durată egală

7 din 20

Înregistrări cu eticheta Qilin [S3]

CE NU REPREZINTĂ

Rată de succes sau atribuire verificată a incidentelor publice

250

Domenii candidate selectate în douăsprezece grupe sectoriale [S2]

CE NU REPREZINTĂ

Clasament oficial, persoane juridice independente sau prevalență națională

50/100 (B)

Valoarea națională Atlas pentru portofoliul selectat [S2]

CE NU REPREZINTĂ

Procent de încălcări, probabilitate de incident sau clasament sectorial

94,8%

Penetrarea internetului în estimarea DataReportal pentru octombrie 2026 [S5]

CE NU REPREZINTĂ

Proporția atacată sau care utilizează servicii sigure

94

Carduri asociate României, vizibile în clar în postările păstrate [S4]

CE NU REPREZINTĂ

Furt de carduri, valabilitate, pierderi sau acoperirea mai largă Brandefense

CONCLUZII PRINCIPALE

01

Verificați conturile și documentele înainte de a accepta afirmațiile unui anunț.

02

Tratați recuperarea, notificarea furnizorilor și prevenirea fraudei drept decizii de afaceri legate între ele.

03

Păstrați separat postările, înregistrările, cazurile oficiale și persoanele.

Harta raportului

Începeți cu decizia care revine rolului dumneavoastră. Urmăriți dovezile până la limitele lor, apoi folosiți capitolul 12 pentru a stabili dovezile de finalizare.

Consiliu și conducere	Finanțarea controlului identității și a recuperării demonstrate	Mergi la 1 5 11 12
CISO	Priorități pentru conturi, furnizori și servicii	Mergi la 3 4 5 7
SOC și infrastructură	Verificarea accesului, poștei și serviciilor	Mergi la 3 4 6 7
Fraudă și relații cu clienții	Respingerea instrucțiunilor neautorizate bazate pe informații autentice	Mergi la 8 9 12
Juridic și comunicare	Aplicarea termenului corect și păstrarea incertitudinii	Mergi la 5 6 10

CAPITOLUL 02

Contextul digital și de securitate al României

02

ÎNTREBAREA ACESTUI CAPITOL

Ce dependențe conturează un răspuns proporțional în România?

94,8%

penetrarea estimată a internetului în octombrie 2026

2.1 Conectivitatea creează multe limite de verificare a identității 11

2.2 Serviciile comune leagă organizații separate 11

2.3 Alegeri și teme regionale: păstrarea limitelor atribuirii 12

2.4 Folosirea datelor publicării fără rescrierea incidentului 12

2.5 Separarea rolurilor naționale de raportare 12

CAPITOLUL 02

Contextul digital și de securitate al României

PE SCURT

O populație conectată pe scară largă depinde de sisteme comune de identitate, plăți și servicii publice. Dovezile acoperă evidențe ale clienților, documente ale furnizorilor, acces la distanță și poștă guvernamentală. Continuitatea și confidențialitatea cer dovezi separate. Cercetarea internațională poate orienta controalele fără să confirme o victimă din România. Cartografiați împreună serviciile importante, administratorii și furnizorii și stabiliți ruta de raportare înaintea unui incident.

2.1 Conectivitatea creează multe limite de verificare a identității

DataReportal estimează 17,8 milioane de utilizatori de internet și o penetrare de 94,8% în octombrie 2026. Raportează 26,1 milioane de conexiuni mobile și 13,6 milioane de identități de utilizator pe rețele sociale. Conexiunile și identitățile sunt unități diferite; niciuna nu reprezintă clienți unici. [S5]

Pentru planificarea securității contează punctul în care un serviciu acceptă autoritatea unei persoane. Un cont de client, un apel la asistență, autentificarea unui furnizor și o sesiune administrativă cer verificări diferite. Cunoașterea datelor personale nu autorizează schimbarea metodei de recuperare sau a destinației unei plăți.

Ofertele comerciale și de documente din capitolul 4 ilustrează această distincție. Ele oferă simultan informații și acces. Nu confirmă niciuna dintre afirmații. Apărătorii trebuie să verifice separat autenticitatea înregistrării, funcționarea autentificării și existența unei acțiuni neautorizate.

2.2 Serviciile comune leagă organizații separate

Contractele turistice, informațiile de facturare și documentele juridice pot trece prin mai multe organizații. O copie poate exista la un furnizor, client, angajat sau consilier extern. Lista contrapărților prezentată de vânzător nu localizează pierderea inițială. [S1]

Cartografiați dependența de serviciu înainte de alegerea răspunsului. Responsabilul aplicației poate identifica exporturile și utilizatorii delegați. Achizițiile pot identifica obligațiile contractuale privind dovezile. Responsabilul cu protecția datelor poate evalua consecințele pentru persoane. Responsabilul contului poate investiga sesiunile.

Acesta este un model analitic de răspuns, nu afirmația că vânzătorii observați au același lanț de furnizori. Ofertele nu sunt legate de un operator sau o sursă comună doar pentru că descriu înregistrări similare.

Comunicarea unui grup de comerț din 19 octombrie a confirmat activitate malițioasă și opriri preventive la mărci din Europa și Statele Unite. Magazinele au rămas deschise; majoritatea site-urilor și aplicațiilor din Europa Centrală și de Sud-Est erau din nou disponibile. Nu identifică servicii românești anume sau o compromitere în România. Apartenența la grup ridică o întrebare despre dependențe, nu confirmă un incident local. [S86]

2.3 Alegeri și teme regionale: păstrarea limitelor atribuirii

Raportul nu adoptă o poziție privind alegerile prezidențiale din noiembrie 2024 anulate, reluarea scrutinului în 2025, candidați, partide sau decizii guvernamentale. Acele alegeri istorice nu stabilesc cauza, autorul sau motivul vreunui incident din 2026 analizat aici.

Referirile la Rusia, Moldova, Ucraina sau Ungaria servesc atribuirii către surse ori contextului de comparație precizat. O postare în rusă nu stabilește naționalitatea sau coordonarea de către un stat. Apropierea regională nu stabilește o campanie comună.

Țările de comparație au fost selectate ca exemple doar pentru a oferi context; alegerea lor nu implică un clasament sau o evaluare politică.

ESET atribuie Cereal grupării Turla cu încredere ridicată. SRI atribuie atacul asupra poștei guvernamentale grupării Turla în propria relatare. Și operațiunea privind routerele din aprilie are o atribuire oficială. Acestea sunt evaluările surselor, nu atribuiri independente noi ale raportului. [S6][S7][S9]

2.4 Folosirea datelor publicării fără rescrierea incidentului

O comunicare din noiembrie poate descrie un eveniment mai vechi, o investigație încheiată sau o evaluare nou publicată. Secțiunea recentă identifică astfel ce a devenit public în perioada finală. Nu mută tacit data intruziunilor anterioare.

În cazul Exchange, ESET indică un început în decembrie 2025 și activitate în ianuarie 2026. SRI afirmă că a identificat atacul în decembrie 2025. Publicările din noiembrie sunt relevante pentru interval, cu păstrarea explicită a cronologiei anterioare. [S6][S7][S8]

Și o sancțiune poate fi emisă după faptele examinate. Data publicării determină includerea în registrul comunicărilor. Când data atacului nu este precizată, raportul nu o inventează și nu o introduce într-o serie lunară de atacuri.

2.5 Separarea rolurilor naționale de raportare

Cadrul românesc de securitate cibernetică civilă desemnează DNSC drept autoritate națională competentă. Cadrul conține excluderi specifice și un tratament distinct pentru entitățile financiare supuse DORA. Raportarea privind datele personale rămâne o întrebare separată. [S13][S14]

Centrul Național Cyberint al SRI furnizează relatările oficiale despre răspunsul privind poșta guvernamentală și operațiunea privind routerele din aprilie. Poliția și procurorii descriu investigații și presupuse fapte. ANSPDCP publică constatări privind protecția datelor. Sursele răspund unor întrebări diferite, iar cifrele lor nu formează un total național de atacuri. [S7][S9][S20]

Capitolul 10 transformă aceste distincții în decizii de raportare. Coordonatorul incidentului trebuie să cunoască entitatea juridică, serviciul și supraveghetorul relevant înaintea primei alerte, cu un contact de rezervă disponibil în afara programului.

CONCLUZII PRINCIPALE

01

Cartografiați serviciile, furnizorii și identitățile înainte de alegerea măsurilor de limitare.

02

Păstrați cronologia evenimentului inițial când folosiți publicări recente.

03

Atribuiți evaluările despre state surselor și excludeți pozițiile politice din analiză.

CAPITOLUL 03

Expunerea națională: domenii de organizații selectate

03

ÎNTREBAREA ACESTUI CAPITOL

Ce observații poate susține această ediție pentru domeniile românești selectate?

250

domenii candidate în douăsprezece grupe sectoriale

3.1 Fișa populației 15

3.2 Observații privind expunerea și valoarea națională Atlas 16

3.3 Observații pasive privind e-mailul 18

3.4 Observații privind DNS, TLS și paginile principale 20

3.5 Verificarea expunerii prin dovezi locale 20

CAPITOLUL 03

Expunerea națională: domenii de organizații selectate

PE SCURT

79 dintre cele 250 de domenii selectate aveau date de autentificare oferite la vânzare. Valoarea națională Atlas este 50/100 (B). Portofoliul înregistrează cel puțin 356.395 de asocieri de dispozitive și 1.355.738 de evidențe de autentificare. Aceste populații suprapuse nu reprezintă persoane unice sau intruziuni confirmate. Controalele pasive păstrează numitorii evaluați. Desemnați responsabili pentru verificarea conturilor curente, investigarea dispozitivelor angajaților și recuperarea serviciilor.

3.1 Fișa populației

Element	Limită
Populație	250 de domenii candidate selectate în douăsprezece grupe sectoriale
Selecție	Instituții publice, servicii financiare, furnizori de servicii esențiale și organizații private importante
Unitate	Domeniu candidat; independența organizațională și proprietatea juridică nu sunt stabilite pentru fiecare intrare
Limita selecției	Portofoliu ales deliberat, nu clasament oficial sau eșantion național reprezentativ
Dată	Observații privind expunerea și controalele pasive din 22 noiembrie 2026 [S2]
Publicare	Valoarea națională Atlas și numărul anonim al semnalelor sectoriale
Interpretare	Observațiile necunoscute nu sunt valori zero sau dovada unei configurații sigure

Populația sectorială apare mai jos. Dimensiunea descrie portofoliul selectat, nu ponderea sectorului în economia României.

Sector	Domenii candidate
Administrație	50
Servicii bancare și financiare	30
Educație	25

Sector	Domenii candidate
Producție și industrie	25
Energie și utilități	20
Comerț și grupuri	20
Transport și logistică	20
Telecom și tehnologie	15
Sănătate	10
Asigurări	10
Ospitalitate și turism	10
Media și divertisment	15
Total	250

Termenul organizație descrie scopul selecției. Numitorul numeric este domeniul candidat. În c03, `orgs_listed_for_sale_now` numără domeniile candidate cu oferte curente; nu stabilește organizații independente. Fișierul descărcabil indică `listing_count_unit` ca `candidate_domains`. Un site de grup poate servi mai multe entități, iar un domeniu corporativ global poate include activitate din afara României. Aceste limite preced orice comparație sectorială.

3.2 Observații privind expunerea și valoarea națională Atlas

79 dintre cele 250 de domenii selectate aveau date de autentificare oferite la vânzare. Valoarea națională Atlas este 50/100 (B), pentru portofoliul selectat. Nu reprezintă procentul de încălcări, probabilitatea unui incident sau certificarea eficacității controalelor. [S2]

Instantaneul expunerii este datat 22 noiembrie 2026. Contextul anual al mențiunilor acoperă 23 noiembrie 2025–22 noiembrie 2026, iar observațiile domeniilor similare acoperă un interval recent de 30 de zile. Semnalele nu reprezintă exclusiv evenimente noi din 2026.

Se publică numai evaluarea națională Atlas. Rândurile sectoriale anonime descriu numărul semnalelor și numitorii domeniilor. Site-urile de grup, serviciile comune și domeniile globale pot include entități asociate sau activitate din afara României.

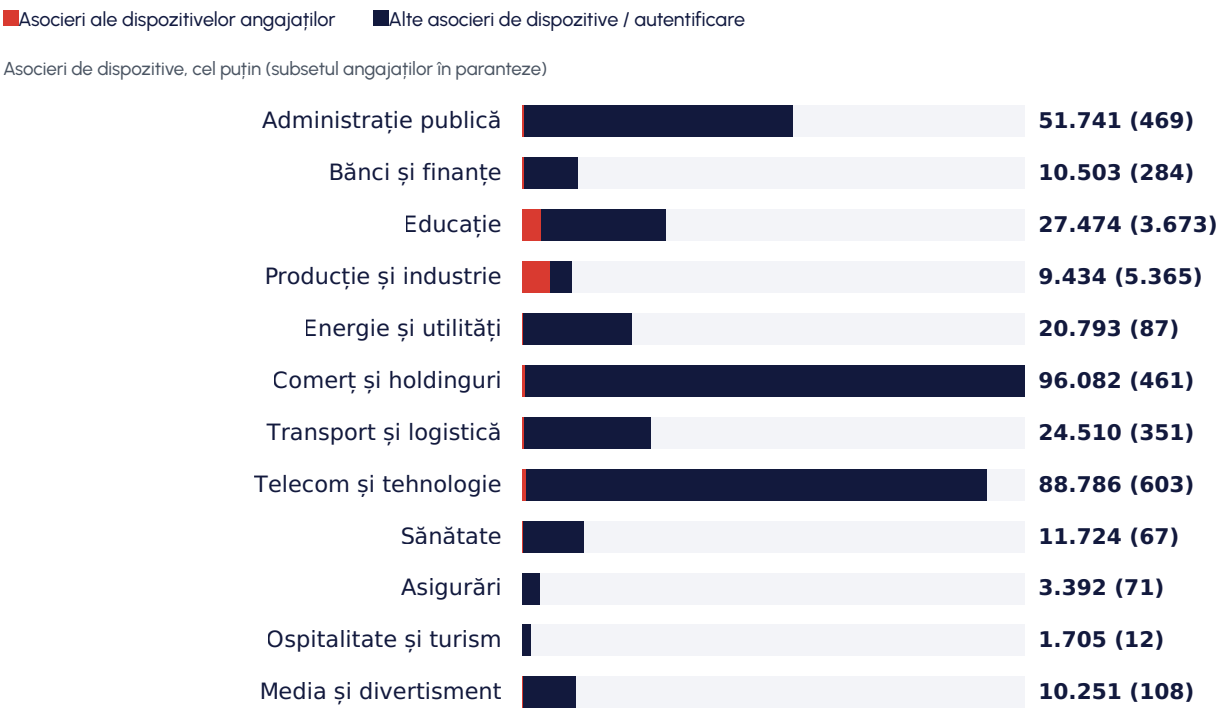
Portofoliul conține cel puțin 356.395 de asocieri de dispozitive, inclusiv 11.551 de asocieri ale dispozitivelor angajaților, și 1.355.738 de evidențe de autentificare. Populațiile se suprapun și nu se adună sau interpretează drept persoane unice. [S2]

Asocierile dispozitivelor privesc 222 de domenii, cele ale angajaților 180, iar evidențele de autentificare 241. Referințele documentelor privesc 102 domenii și totalizează 568 de observații. Domeniile similare candidate privesc 169 de domenii; nu reprezintă infrastructură malițioasă verificată. [S2]

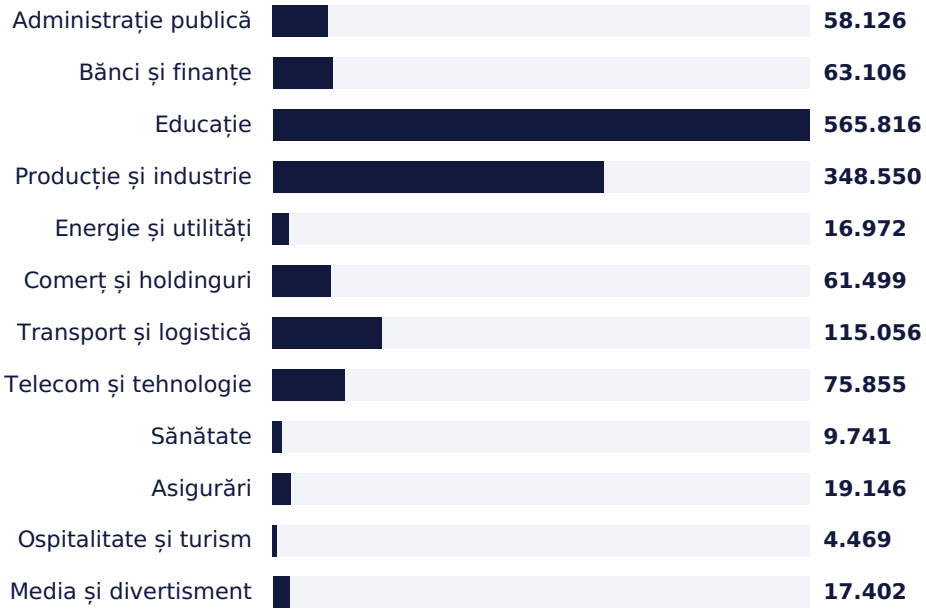
Tabelul prezintă asocierile dispozitivelor ca numere minime observate. Evidențele de autentificare reunesc populații istorice și nu stabilesc parole valide, infectare curentă sau utilizatori exclusiv din România.

Sector	Domenii	Oferte curente	Asocieri dispozitive	Evidențe autentificare
Administrație	50	9	51.741	58.126
Servicii bancare și financiare	30	9	10.503	63.106
Educație	25	6	27.474	565.816
Producție și industrie	25	4	9.434	348.550
Energie și utilități	20	8	20.793	16.972
Comerț și grupuri	20	17	96.082	61.499
Transport și logistică	20	3	24.510	115.056
Telecom și tehnologie	15	6	88.786	75.855
Sănătate	10	2	11.724	9.741
Asigurări	10	3	3.392	19.146
Ospitalitate și turism	10	5	1.705	4.469
Media și divertisment	15	7	10.251	17.402
Total	250	79	356.395	1.355.738

Asocierile dispozitivelor și evidențele de autentificare păstrează numitorii sectoriali separați



Asocieri de evidențe de autentificare (scară separată)



Sursa: observații privind expunerea pentru 250 de domenii candidate selectate, 22 noiembrie 2026 [S2]. Asocierile cumulative se pot suprapune și pot include materiale istorice; nu reprezintă persoane unice, intruziuni curente sau prevalență națională.

79 din 250

domenii selectate cu o ofertă curentă de date de autentificare

50/100 (B)

valoarea națională Atlas pentru portofoliul selectat

O ofertă curentă de date de autentificare trebuie să declanșeze investigarea contului. Singură, nu stabilește o parolă funcțională, o intruziune reușită, o vânzare încheiată sau un număr de angajați afectați.

Asocierile de dispozitive cer altă întrebare: al cui este dispozitivul, ce serviciu poate accesa și în ce moment? Clienții, studenții, angajații și identitățile din servicii comune pot utiliza același domeniu corporativ. Asocierea cu domeniul nu clarifică singură proprietatea sau infectarea curentă.

Și evidențele istorice de autentificare cer verificarea contului. O înregistrare poate fi veche, repetată în mai multe surse, deja remediată sau asociată unui client. Nu luați o decizie perturbatoare asupra conturilor pornind doar de la un total cumulativ.

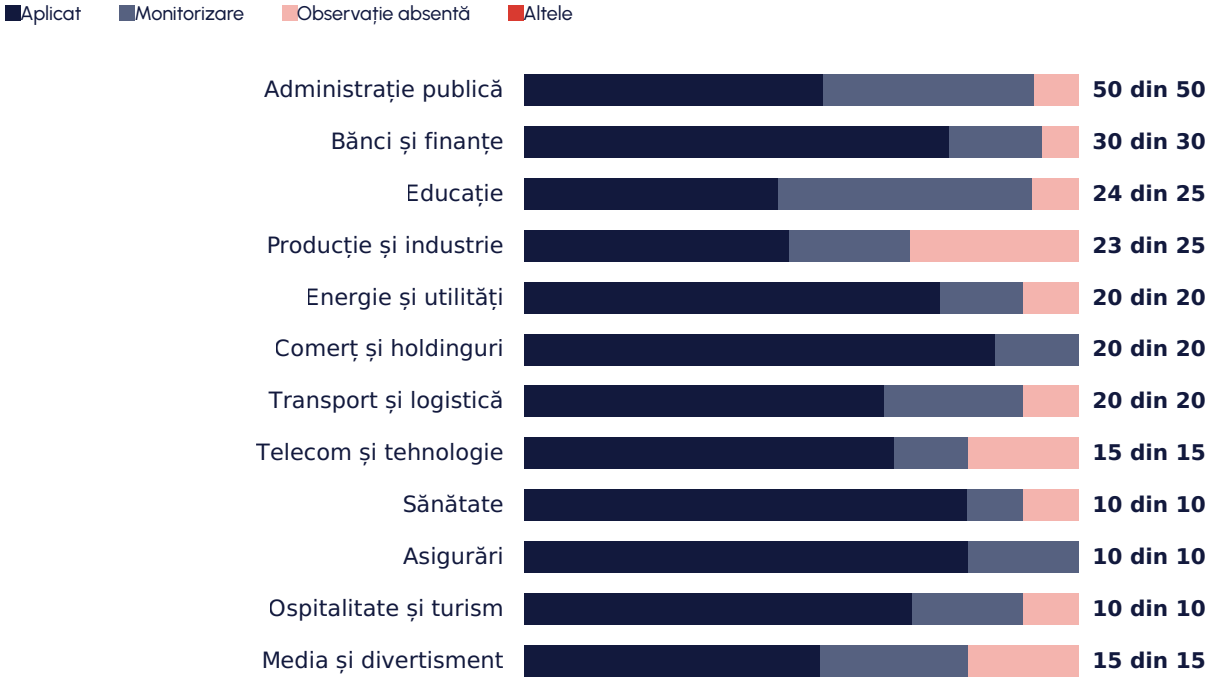
3.3 Observații pasive privind e-mailul

Rezultatele pasive de mai jos își păstrează propriul numitor de observație. Aplicarea DMARC, un record SPF și un record DKIM răspund unor întrebări diferite. O observație absentă sau nereușită nu echivalează cu absența confirmată a controlului. [S2][S18]

Există observații pasive pentru 247 dintre cele 250 de domenii selectate; 3 rămân neevaluate. [S2]

Observație	Număr	Numitor
Aplicare DMARC solicitată	158	247
Monitorizare DMARC	62	247
Record DMARC negăsit	27	247
Altă observație DMARC	0	247
Record SPF găsit	239	247
Record DKIM găsit	177	247

Observațiile politicilor de e-mail păstrează numitorii sectoarelor selectate



Sursa: observații pasive, 22 noiembrie 2026 [S2]. 250 de domenii candidate; 247 de domenii observate. Fiecare sector își păstrează numitorul observațiilor. O observație absentă nu confirmă absența controlului.

DMARC comunică tratamentul cerut de proprietarul domeniului pentru mesajele care nu trec verificările de aliniere a autentificării. O politică de monitorizare nu cere respingerea. Carantina sau respingerea nu garantează aplicarea de către fiecare destinatar ori oprirea impersonării. [S18]

Acțiunea practică este identificarea expeditorilor legitimi, examinarea rapoartelor și introducerea treptată a aplicării politicii împreună cu responsabilul e-mailului. Includeți salarizarea externalizată, asistența, facturarea și marketingul. Schimbarea este finalizată când mesajele legitime rămân utilizabile, iar responsabilul excepțiilor este cunoscut.

3.4 Observații privind DNS, TLS și paginile principale

Dintre cele 247 domenii observate, 31 au o observație de delegare DNSSEC. Există rezultate TLS pentru 217, dintre care 207 erau valide la verificare. Paginile erau accesibile pentru 187; HSTS a fost observat la 124. Numitorii răspund unor întrebări diferite. [S2]

Tratați observația unei delegări DNSSEC drept semnal de delegare, nu validare completă a fiecărui răspuns DNS. Negăsirea unui record DKIM nu demonstrează că organizația nu semnează niciodată mesajele. O pagină accesibilă nu stabilește autorizarea sigură în aplicație.

Observațiile TLS se aplică punctului și datei evaluate. O observație nereușită poate rezulta din disponibilitatea serviciului, prezentarea certificatului sau limite de acces. Examinați serviciul și publicul său vizat înainte de alegerea remedierii.

Implicați responsabilul serviciului. Unele domenii nu au intenționat o aplicație publică sau e-mail de ieșire. Consemnați scopul și configurația aprobate, în loc să impuneți același model operațional fiecărui domeniu.

3.5 Verificarea expunerii prin dovezi locale

Semnal	Prima verificare	Declanșatorul escaladării	Dovada finalizării
Ofertă de autentificare	Cont activ, privilegii și istoricul remedierii	Autentificare neautorizată demonstrată sau acces privilegiat valid	Decizie asupra sesiunii și acceptarea responsabilului
Asociere de dispozitiv	Relația dintre dispozitiv și cont	Infectare activă sau sesiune privilegiată neexplicată	Limitare, analizarea sesiunilor și decizie consemnată
Afirmație privind documente	Evidențe interne autorizate și istoricul accesului	Evidențe sensibile verificate sau export neautorizat	Sfera datelor, decizie juridică și corectarea accesului
Politică de e-mail	Servicii expediatoare și scopul domeniului	Expeditor neaprobat sau lipsă materială de autentificare	Politică aprobată și livrare legitimă testată
Afirmație privind disponibilitatea	Telemetria serviciului și dovezile furnizorului	Perturbare confirmată a unui flux de afaceri	Restabilire acceptată de responsabilul serviciului

Acestea sunt etape recomandate de verificare. Nu descriu modul în care Brandefense construiește o evaluare sau își colectează dovezile.

CONCLUZII PRINCIPALE

01

Numitorul portofoliului este de 250 de domenii candidate, cu limite privind proprietatea și independența.

02

Valoarea națională Atlas descrie acest portofoliu; observațiile pasive păstrează numitori separați.

03

Verificați separat conturile, dispozitivele, documentele și scopul serviciului înainte de a acționa.

CAPITOLUL 04

Ce arată dovezile din mediul clandestin

04

ÎNTREBAREA ACESTUI CAPITOL

Ce stabilesc ofertele de date și acces asociate României și ce trebuie verificat?

4.1 Fișa populației 23
4.2 Volum, platforme și limbi 23
4.3 Cum se citesc dosarele 26
4.4 Cazul A: Oferte de acces la servicii publice (B01) 27
4.5 Cazul B: Redirecționarea unor date vechi de facturare (B02) 28
4.6 Cazul C: Conturi de consumatori și cereri de ocolire a verificării (B03) 29
4.7 Cazul D: Afirmație despre datele clienților unui magazin (B04) 31
4.8 Cazul E: Afirmație despre clienți și facturi din servicii IT (B05) 32
4.9 Cazul F: Afirmații despre marketing digital și CRM (B06) 33
4.10 Cazul G: Ofertă de date personale cu fotografii (B07) 35
4.11 Cazul H: Afirmație privind contracte de servicii turistice (B08) 36
4.12 Cazul I: Oferta din mai privind date ale clienților (B09) 37
4.13 Cazul J: Afirmație despre salarizare în educație (B10) 39
4.14 Cazul K: Oferta din iunie privind date ale clienților (B11) 40
4.15 Cazul L: Ofertă de documente ale unor servicii juridice private (B12) 41
4.16 Cazul M: Ofertă de acces administrativ la o platformă comercială (B13) 43
4.17 Alte oferte de servicii și limite 44
4.18 Cazul N: Ofertă de documente de identitate și liste de pasageri din aviația privată (B24) 45

14 dosare detaliate de anunțuri, cu limite distincte ale dovezilor

CAPITOLUL 04

Ce arată dovezile din mediul clandestin

PE SCURT

Materialul de forum păstrat oferă acces, evidențe despre clienți, documente și servicii de identitate. Unele postări se referă la date vechi; ofertele recente privesc administrarea unei platforme comerciale și documente juridice. Dosarele de mai jos stabilesc ce s-a oferit, nu autenticitatea accesului sau volumului pretins. Verificați proprietatea contului, actualitatea datelor și exporturile autorizate înainte de a decide limitarea, protecția clienților sau notificarea.

4.1 Fișa populației

Element	Limită
Interval	1 ianuarie–22 noiembrie 2026, după data postării
Populație etichetată cu țara	773.764 postări [S1]
Arhivă păstrată	41.379 postări distincte [S1]
Populația de forum	256 de postări etichetate cu țara, păstrate în unsprezece luni
Populație recentă de forum	14 postări din 8–22 noiembrie
Unitatea cazului	Un dosar editorial poate conține mai multe anunțuri sau răspunsuri
Limita dovezilor	Textul observat nu autentifică o bază, un cont funcțional sau o vânzare

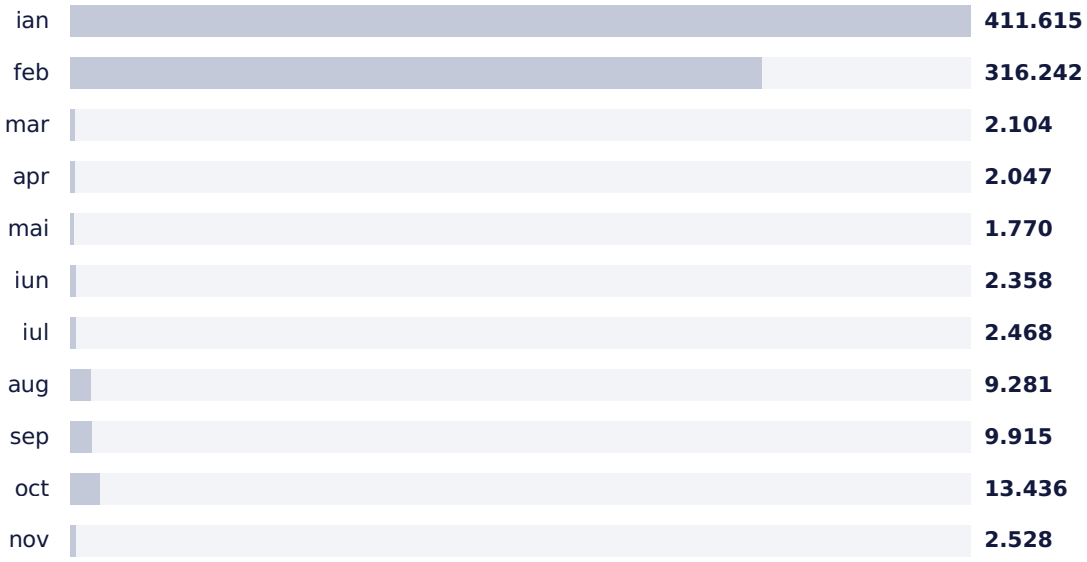
Etichetele de țară descriu relația materialului cu țara. Un catalog de servicii pentru mai multe țări sau o listă de piețe de plăți nu confirmă vizarea României. Răspunsurile, republicările, anunțurile și bazele pretinse sunt obiecte diferite.

4.2 Volum, platforme și limbi

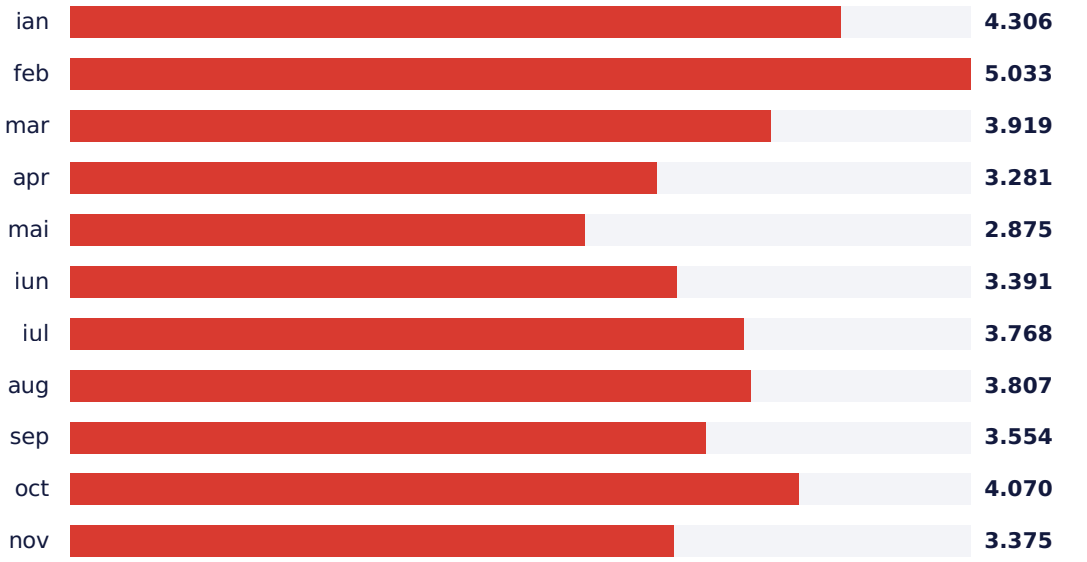
Populația etichetată cu țara este de 773.764 postări. Ianuarie reprezintă 411.615, adică 53,2%. Arhiva raportului conține 41.379 postări distincte. Sunt măsuri ale vizibilității, nu o serie de incidente. Populația păstrată nu acoperă fiecare postare etichetată. [S1]

Volumele lunare ale postărilor descriu vizibilitatea, nu tendința atacurilor

Postări etichetate România



Arhiva păstrată (scară separată)



Sursa: Brandefense Blackhole, postări etichetate România și arhiva păstrată, 1 ianuarie–22 noiembrie 2026; ultima zi este parțială. Postările nu sunt atacuri sau incidente unice [S1].

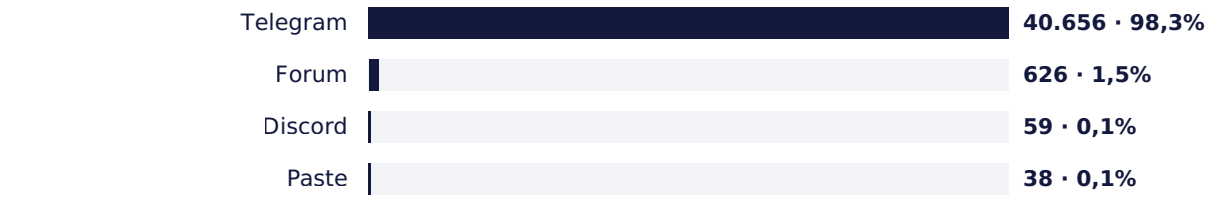
Perspectivă	Etichetă	Postări	Numitorul arhivei
Platformă	forum	626	41.379
Platformă	discord	59	41.379
Platformă	telegram	40.656	41.379
Platformă	paste	38	41.379
Limbă	EN	17.442	41.379

Perspectivă	Etichetă	Postări	Numitorul arhivei
Limbă	RU	10.524	41.379
Limbă	TR	4.422	41.379
Limbă	ID	2.752	41.379
Limbă	RO	954	41.379
Limbă	UK	735	41.379
Limbă	ZH	515	41.379
Limbă	ES	280	41.379

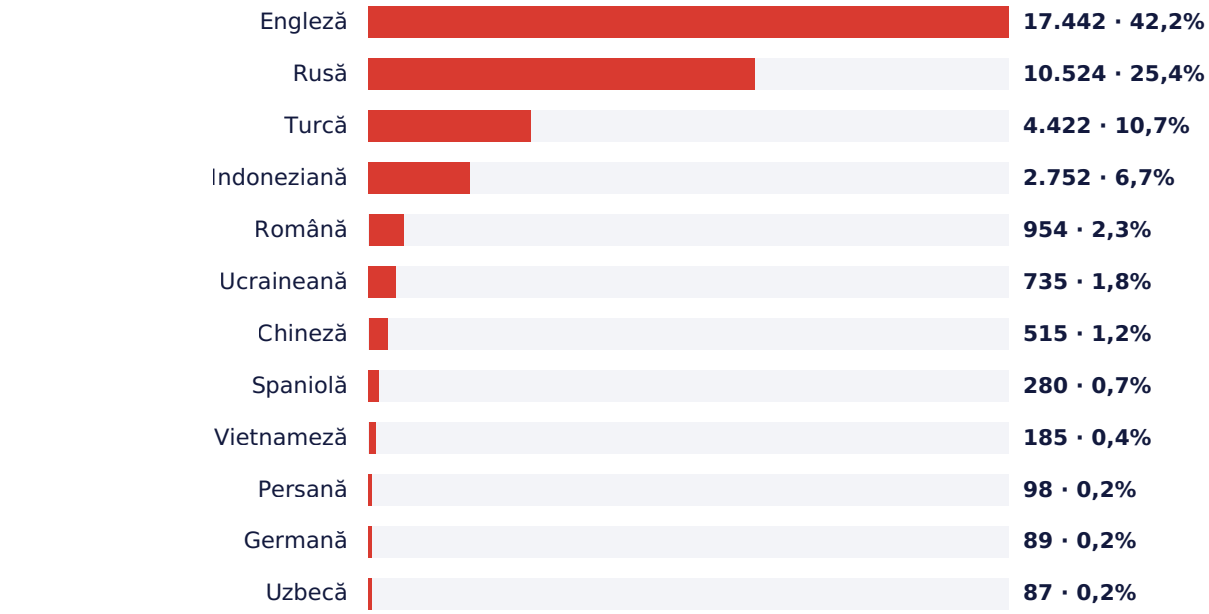
Observațiile limbilor se pot suprapune; rândurile nu se adună ca postări distincte. Platformele descriu arhiva păstrată, nu întreaga populație etichetată cu țara. [S1]

Observațiile platformelor și limbilor păstrează numitori separați

Observații privind platformele / 41.379 de postări păstrate



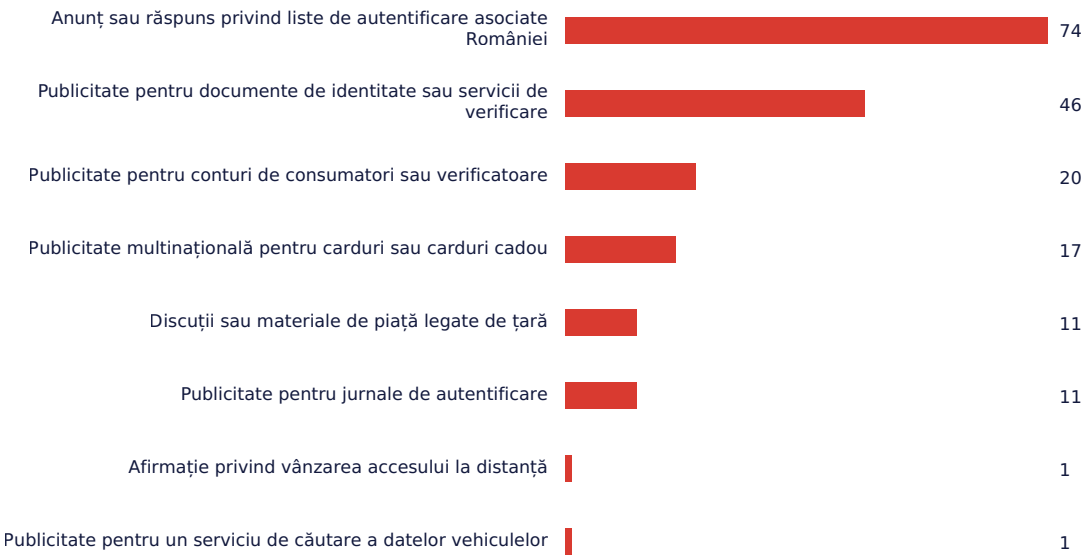
Observații privind limbile / 41.379 de postări păstrate



Etichetele de limbă se pot suprapune; platformele și limbile sunt perspective separate asupra arhivei păstrate. Sursa: Brandefense Blackhole, postări etichetate România și arhiva păstrată, 1 ianuarie–22 noiembrie 2026; ultima zi este parțială. Postările nu sunt atacuri sau incidente unice [S1].

Arhiva și perspectiva națională etichetată au acoperiri diferite. Nu sunt prezentate ca populații incluse una în alta. Repetiția, publicitatea și vizibilitatea inegală împiedică interpretarea volumului drept schimbare a prevalenței naționale a incidentelor.

Alte teme ale forumului etichetate cu țara descriu postări, nu incidente verificate



Baza: 256 de postări de forum păstrate, etichetate pe țară; temele descriu conținutul, nu incidente verificate. Sursa: Brandefense Blackhole, postări etichetate România și arhiva păstrată, 1 ianuarie–22 noiembrie 2026; ultima zi este parțială. Postările nu sunt atacuri sau incidente unice [S1].

4.3 Cum se citesc dosarele

Fiecare caz reunește afirmația, cronologia, dovezile deținute, alternativele și răspunsul. Un răspuns interesat nu este validare independentă. Formularea similară nu dovedește același fișier sau operator. Data indicată de sursă rămâne o afirmație dacă nu este coroborată independent.

Activitatea observată include vânzarea accesului, promovarea bazelor de date, documente de identitate, servicii pentru conturi de consumatori și recircularea datelor istorice. Temele descriu conținutul. Nu împart incidentele României în categorii exhaustive și nu măsoară veniturile infractorilor. [S1]

4.4 Cazul A: Oferte de acces la servicii publice (B01)

CAZUL A

A

Oferte de acces la servicii publice

Fișă de dovezi B01 | 1 ian 2026 | Forum | Administrație

Anunț neverificat

AFIRMAȚIE	Două postări oferă acces nespecificat la portaluri prezentate ca guvernamentale românești. Formulări similare apar sub două pseudonime. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-01-01, 2026-06-01. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.
ALTERNATIVĂ	Un anunț copiat sau o ofertă fictivă poate explica formularea similară. Nu atribuiți identitatea sau accesul doar pe baza textului.
LIMITĂ	Nu sunt stabilite portalul, contul, accesul funcțional, o vânzare sau un operator comun. A doua postare nu demonstrează o altă intruziune.
RĂSPUNS	Verificați accesul privilegiat la serviciile publice și dovezile sesiunilor înainte de măsuri perturbatoare.
DECIZIE	Consemnați decizia responsabilului serviciului. Dacă nu există un cont sau sistem corespondent, păstrați incertitudinea fără a numi o platformă națională.

Concluzie

Nu sunt stabilite portalul, contul, accesul funcțional, o vânzare sau un operator comun. A doua postare nu demonstrează o altă intruziune.

Fișă de dovezi B01 — 1 ian 2026

renquix | Forum | Forum | EN

ORIGINAL

Selling romanian gov portal access

TRADUCERE

Vând acces la un portal guvernamental românesc

Ce este documentat

Două postări oferă acces nespecificat la portaluri prezentate ca guvernamentale românești. Formulări similare apar sub două pseudonime.

Ce nu este stabilit

Nu sunt stabilite portalul, contul, accesul funcțional, o vânzare sau un operator comun. A doua postare nu demonstrează o altă intruziune.

4.5 Cazul B: Recircularea unor date vechi de facturare (B02)

B

CAZUL B

Recircularea unor date vechi de facturare

Fișă de dovezi B02 | 21 ian 2026 | Forum | Servicii de afaceri

Anunț neverificat

AFIRMAȚIE	Postări din ianuarie și martie recirculă baze pretinse de facturare și clienți. Descrierile indică proveniență din 2023 sau 2024 și volume diferite. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-01-21, 2026-01-23, 2026-03-22. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.
ALTERNATIVĂ	Recircularea unui export vechi poate explica publicarea recentă. O etichetă recentă nu schimbă automat vechimea datelor.
LIMITĂ	Afirmațiile nu datează o intruziune nouă în 2026. Volumele diferite nu stabilesc identitatea fișierelor. Eșantioanele nu au fost validate independent.
RĂSPUNS	Verificați dacă identitățile și secretele relevante au fost deja remediate. Stabiliți actualitatea înainte de răspuns.

DECIZIE	Verificați schimbarea parolelor și tokenurilor după perioada pretinsă. O listă istorică poate susține impersonarea chiar dacă parolele vechi nu mai funcționează.

Concluzie

Afirmațiile nu datează o intruziune nouă în 2026. Volumele diferite nu stabilesc identitatea fișierelor. Eșantioanele nu au fost validate independent.

Fișă de dovezi B02 21 ian 2026

EchoEcho Forum Forum EN

ORIGINAL

SQL dump (2.08GB sql files) 04.2024 clients - 209K lines

TRADUCERE

Export SQL (fișiere SQL de 2,08 GB), 04.2024, clienți: 209K linii

Ce este documentat

Postări din ianuarie și martie recirculă baze pretinse de facturare și clienți. Descrierile indică proveniență din 2023 sau 2024 și volume diferite.

Ce nu este stabilit

Afirmațiile nu datează o intruziune nouă în 2026. Volumele diferite nu stabilesc identitatea fișierelor. Eșantioanele nu au fost validate independent.

4.6 Cazul C: Conturi de consumatori și cereri de ocolire a verificării (B03)

C

CAZUL C

Conturi de consumatori și cereri de ocolire a verificării

Fișă de dovezi B03 16 feb 2026 Forum Servicii pentru consumatori

Anunț neverificat

AFIRMAȚIE	În cursul anului apar liste de conturi de pariuri asociate țării și cereri ori oferte de instrumente pentru verificarea conturilor și a identității. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-01-24, 2026-02-12, 2026-02-16, 2026-09-24, 2026-10-11. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.

ALTERNATIVĂ	O cerere de cumpărare poate reflecta interes fără produs disponibil. Un instrument promovat poate să nu funcționeze în serviciul curent.
LIMITĂ	O cerere nu demonstrează existența capacității. Nu sunt stabilite ocolirea funcțională, accesul testat, o intruziune nouă sau frauda încheiată.
RĂSPUNS	Urmăriți autentificările automate, modificarea înscrierii și recuperarea conturilor. Testați verificarea față de documente reutilizate.
DECIZIE	Testați recuperarea și înscrierea prin exerciții autorizate. Verificarea identității cere mai mult decât recunoașterea unor date personale.

Concluzie

O cerere nu demonstrează existența capacității. Nu sunt stabilite ocolirea funcțională, accesul testat, o intruziune nouă sau frauda încheiată.

Fișă de dovezi B03 16 feb 2026

Reddington66 Forum Forum EN

ORIGINAL

want to buy a kyc bypass

TRADUCERE

vreau să cumpăr o metodă de ocolire a verificării identității

Ce este documentat

În cursul anului apar liste de conturi de pariuri asociate țării și cereri ori oferte de instrumente pentru verificarea conturilor și a identității.

Ce nu este stabilit

O cerere nu demonstrează existența capacității. Nu sunt stabilite ocolirea funcțională, accesul testat, o intruziune nouă sau frauda încheiată.

4.7 Cazul D: Afirmație despre datele clienților unui magazin (B04)

CAZUL D

D

Afirmație despre datele clienților unui magazin

Fișă de dovezi B04 | 4 mar 2026 | Forum | Comerț

Anunț neverificat

AFIRMAȚIE	O postare din martie descrie o bază de date a unui magazin online românesc, cu informații despre clienți și companii. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-03-04. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.
ALTERNATIVĂ	Datele ar putea proveni dintr-un export istoric sau de la un furnizor. Descrierea vânzătorului nu localizează pierderea inițială.
LIMITĂ	Nu sunt stabilite originea, accesul curent, caracterul complet sau mecanismul pretins al intruziunii.
RĂSPUNS	Examinați accesul la conturi și baze de date, păstrați jurnalele și decideți notificarea pe baza înregistrărilor validate.
DECIZIE	Cereți reconcilierea exporturilor, utilizatorilor delegați și retenției. Expresia date complete despre clienți nu demonstrează expunerea cardurilor.

Concluzie

Nu sunt stabilite originea, accesul curent, caracterul complet sau mecanismul pretins al intruziunii.

Fișă de dovezi B04 4 mar 2026

Eliphas Forum Forum EN

ORIGINAL

Romanian online store with full customer data

TRADUCERE

Magazin online românesc, cu date complete despre clienți

Ce este documentat

O postare din martie descrie o bază de date a unui magazin online românesc, cu informații despre clienți și companii.

Ce nu este stabilit

Nu sunt stabilite originea, accesul curent, caracterul complet sau mecanismul pretins al intruziunii.

4.8 Cazul E: Afirmație despre clienți și facturi din servicii IT (B05)

E

CAZUL E

Afirmație despre clienți și facturi din servicii IT

Fișă de dovezi B05 | 2 apr 2026 | Forum | Tehnologie

Anunț neverificat

AFIRMAȚIE	O postare din aprilie oferă peste 300.000 de înregistrări despre clienți, angajați și facturi, cu un volum pretins de 1,95 GB. Un răspuns cere vizualizarea materialului. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-04-02, 2026-04-02. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.
ALTERNATIVĂ	Un export poate combina mai multe tipuri de tabele. Facturile și clienții au unități diferite, chiar într-un fișier autentic.
LIMITĂ	Rândurile pretinse nu sunt victime unice. Răspunsul nu confirmă independent materialul și nu demonstrează transferul.
RĂSPUNS	Verificați accesul furnizorilor de servicii, schimbările facturilor și confirmarea contactelor partenerilor.

DECIZIE	Tratați factura familiară drept context, nu autoritate de plată. Confirmați modificarea beneficiarului printr-un contact cunoscut anterior.

Concluzie

Rândurile pretinse nu sunt victime unice. Răspunsul nu confirmă independent materialul și nu demonstrează transferul.

Fișă de dovezi B05 2 apr 2026

xorcat Forum Forum EN

ORIGINAL

Records: 300,000+ client records, employees, invoices

TRADUCERE

Înregistrări: peste 300.000 de înregistrări despre clienți, angajați și facturi

Ce este documentat

O postare din aprilie oferă peste 300.000 de înregistrări despre clienți, angajați și facturi, cu un volum pretins de 1,95 GB. Un răspuns cere vizualizarea materialului.

Ce nu este stabilit

Rândurile pretinse nu sunt victime unice. Răspunsul nu confirmă independent materialul și nu demonstrează transferul.

4.9 Cazul F: Afirmații despre marketing digital și CRM (B06)

F

CAZUL F

Afirmații despre marketing digital și CRM

Fișă de dovezi B06 | 7 apr 2026 | Forum | Servicii de afaceri

Anunț neverificat

AFIRMAȚIE	Postări din aprilie oferă o bază de marketing digital și informații din servicii CRM sau de mesagerie. Una pretinde peste 40.000 de rânduri. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-04-04, 2026-04-07. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.
ALTERNATIVĂ	Un export comercial ori o copie de la un partener poate explica materialul. Disputa dintre pseudonime nu rezolvă proveniența.

LIMITĂ	Acuzația unui autor că alt pseudonim republică date nu dovedește autorul inițial, identitatea fișierului sau un operator comun. Valabilitatea accesului și originea materialului oferit rămân neverificate.
RĂSPUNS	Rotiți secretele de integrare a căror expunere este validată, examinați autorizările și păstrați jurnalele serviciilor de mesagerie.
DECIZIE	Limita răspunsului este integrarea validată și permisiunile sale. Resetarea întregii organizații cere dovezi suplimentare față de anunț.

Concluzie

Acuzația unui autor că alt pseudonim republică date nu dovedește autorul inițial, identitatea fișierului sau un operator comun. Valabilitatea accesului și originea materialului oferit rămân neverificate.

Fișă de dovezi B06 7 apr 2026

xorcat Forum Forum EN

ORIGINAL

Records: 40,000+ rows

TRADUCERE

Înregistrări: peste 40.000 de rânduri

Ce este documentat

Postări din aprilie oferă o bază de marketing digital și informații din servicii CRM sau de mesagerie. Una pretinde peste 40.000 de rânduri.

Ce nu este stabilit

Acuzația unui autor că alt pseudonim republică date nu dovedește autorul inițial, identitatea fișierului sau un operator comun. Valabilitatea accesului și originea materialului oferit rămân neverificate.

4.10 Cazul G: Ofertă de date personale cu fotografii (B07)

CAZUL G

G

Ofertă de date personale cu fotografii

Fișă de dovezi B07 | 20 mar 2026 | Forum | Servicii de identitate

Anunț neverificat

AFIRMAȚIE	O ofertă din martie pretinde o bază cu 8.000 de cetățeni români și fotografii. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-03-20. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.
ALTERNATIVĂ	O colecție ar putea reuni date din mai multe surse. Cuvântul cetățeni nu demonstrează originea într-un sistem al statului.
LIMITĂ	Titlul este un anunț. Nu sunt stabilite sistemul sursă, populația, consimțământul, caracterul complet sau data obținerii.
RĂSPUNS	Verificați recuperarea identității față de date personale cunoscute și imagini reutilizate. Nu presupuneți un incident la un registru național.
DECIZIE	Examinați recuperarea conturilor, reutilizarea documentelor și permisiunile excesive de căutare. Protejați persoanele fără a prezenta totalul pretins ca populație verificată.

Concluzie

Titlul este un anunț. Nu sunt stabilite sistemul sursă, populația, consimțământul, caracterul complet sau data obținerii.

Fișă de dovezi B07 — 20 mar 2026

fent888 | Forum | Forum | EN

ORIGINAL

Romania Database 8k Citizens + Photo

TRADUCERE

Bază de date cu 8k cetățeni români și fotografii

Ce este documentat

O ofertă din martie pretinde o bază cu 8.000 de cetățeni români și fotografii.

Ce nu este stabilit

Titlul este un anunț. Nu sunt stabilite sistemul sursă, populația, consimțământul, caracterul complet sau data obținerii.

4.11 Cazul H: Afirmație privind contracte de servicii turistice (B08)

CAZUL H

H

Afirmație privind contracte de servicii turistice

Fișă de dovezi B08 | 24 apr 2026 | Forum | Turism

Anunț neverificat

AFIRMAȚIE	O postare din aprilie pretinde contracte turistice și amenință cu publicarea altor liste de cazare și rezervări. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-04-24. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.
ALTERNATIVĂ	Un document poate exista legitim la mai multe contrapărți. Menționarea unui hotel nu demonstrează o intruziune în sistemele sale.
LIMITĂ	Discuția ulterioară nu oferă confirmare independentă. Autenticitatea și amploarea documentelor rămân neverificate.
RĂSPUNS	Examinați partajarea documentelor cu partenerii turistici și revocați accesul doar după validarea unei corespondențe.

DECIZIE	Protejați separat rezervările, comunicarea cu oaspeții și instrucțiunile de plată. Confirmați modificările printr-un canal cunoscut, nu contactul din mesajul suspect.

Concluzie

Discuția ulterioară nu oferă confirmare independentă. Autenticitatea și amploarea documentelor rămân neverificate.

Fișă de dovezi B08 24 apr 2026

johnapp Forum Forum EN

ORIGINAL

leaks of confidential contracts with other chain hotels

TRADUCERE

publicarea unor contracte confidențiale cu alte lanțuri hoteliere

Ce este documentat

O postare din aprilie pretinde contracte turistice și amenință cu publicarea altor liste de cazare și rezervări.

Ce nu este stabilit

Discuția ulterioară nu oferă confirmare independentă. Autenticitatea și amploarea documentelor rămân neverificate.

4.12 Cazul I: Oferta din mai privind date ale clienților (B09)

CAZUL I

Oferta din mai privind date ale clienților

Fișă de dovezi B09 | 7 mai 2026 | Forum | Comerț

Anunț neverificat

AFIRMAȚIE	Un vânzător oferă 86.283 de linii pentru 300 USD și atribuie datelor data de 4 mai 2026. Același pseudonim republică anunțul, îl readuce în atenție și primește un răspuns. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-05-07, 2026-05-07, 2026-05-07, 2026-05-12. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.

ALTERNATIVĂ	Publicările repetate pot reprezenta aceeași ofertă. Un preț cerut nu stabilește valoarea realizată sau numărul cumpărătorilor.
LIMITĂ	Data indicată de autor nu este verificată independent. Republicările nu stabilesc intruziuni separate sau vânzări încheiate.
RĂSPUNS	Examinați exporturile de date ale clienților și accesul la conturi. Validați informațiile prin evidențe interne autorizate înainte de notificare.
DECIZIE	Comparați datele validate cu rutele permise de export. Păstrați distincția dintre linii oferite și clienți unici.

Concluzie

Data indicată de autor nu este verificată independent. Republicările nu stabilesc intruziuni separate sau vânzări încheiate.

Fișă de dovezi B09 7 mai 2026

moxzey Forum Forum EN

ORIGINAL

Total lines:86.283

TRADUCERE

Total linii: 86.283

Ce este documentat

Un vânzător oferă 86.283 de linii pentru 300 USD și atribuie datelor data de 4 mai 2026. Același pseudonim republică anunțul, îl readuce în atenție și primește un răspuns.

Ce nu este stabilit

Data indicată de autor nu este verificată independent. Republicările nu stabilesc intruziuni separate sau vânzări încheiate.

4.13 Cazul J: Afirmație despre salarizare în educație (B10)

CAZUL J

J

Afirmație despre salarizare în educație

Fișă de dovezi B10 | 24 mai 2026 | Forum | Educație

Anunț neverificat

AFIRMAȚIE	Un fir din mai și un răspuns care îl citează oferă 331K de înregistrări legate de profesori și date de autentificare administrativă. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-05-24, 2026-05-24. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.
ALTERNATIVĂ	Un export administrativ poate include poziții sau înregistrări repetate. Numărul pretins nu dovedește persoane distincte sau acces în întreaga țară.
LIMITĂ	Sistemul sursă, acoperirea națională, numărul înregistrărilor și accesul curent rămân neverificate. Nu sunt stabilite date de autentificare funcționale.
RĂSPUNS	Examinați privilegiile furnizorilor de salarizare și jurnalele identităților personalului. Validați contul relevant înainte de resetarea unei populații largi.
DECIZIE	Verificați separat permisiunile furnizorului și administratorilor interni. Validați sistemul sursă și contul înainte de extinderea răspunsului.

Concluzie

Sistemul sursă, acoperirea națională, numărul înregistrărilor și accesul curent rămân neverificate. Nu sunt stabilite date de autentificare funcționale.

Fișă de dovezi B10 24 mai 2026

somewhere Forum Forum EN

ORIGINAL

331K TEACHERS + ADMIN CREDS PLAINTEXT

TRADUCERE

331K PROFESORI ȘI DATE DE AUTENTIFICARE ADMINISTRATIVĂ ÎN CLAR

Ce este documentat

Un fir din mai și un răspuns care îl citează oferă 331K de înregistrări legate de profesori și date de autentificare administrativă.

Ce nu este stabilit

Sistemul sursă, acoperirea națională, numărul înregistrărilor și accesul curent rămân neverificate. Nu sunt stabilite date de autentificare funcționale.

4.14 Cazul K: Oferta din iunie privind date ale clienților (B11)

K

CAZUL K

Oferta din iunie privind date ale clienților

Fișă de dovezi B11 | 20 iun 2026 | Forum | Comerț

Anunț neverificat

AFIRMAȚIE	O postare din iunie pretinde 453.009 linii și atribuie presupusului incident data de 19 iunie 2026. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-06-20. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.
ALTERNATIVĂ	Un export vechi, un subset sau un material fabricat rămân explicații posibile. Câmpurile credibile nu autentifică volumul complet.
LIMITĂ	Data pretinsă nu este dovadă independentă. Câmpurile enumerate și rândurile eșantion nu verifică întreaga bază oferită ori originea sa.
RĂSPUNS	Examinați exporturile neobișnuite și accesul la evidențele clienților, apoi evaluați raportarea datelor personale pe baza faptelor validate.

DECIZIE	Stabiliți sfera și momentul luării la cunoștință prin dovezile aplicației. Potrivirea unui eșantion susține investigarea înainte de acceptarea tuturor afirmațiilor.

Concluzie

Data pretinsă nu este dovadă independentă. Câmpurile enumerate și rândurile eșantion nu verifică întreaga bază oferită ori originea sa.

Fișă de dovezi B11 20 iun 2026

tempp991 Forum Forum EN

ORIGINAL

Total lines: 453.009

TRADUCERE

Total linii: 453.009

Ce este documentat

O postare din iunie pretinde 453.009 linii și atribuie presupusului incident data de 19 iunie 2026.

Ce nu este stabilit

Data pretinsă nu este dovadă independentă. Câmpurile enumerate și rândurile eșantion nu verifică întreaga bază oferită ori originea sa.

4.15 Cazul L: Ofertă de documente ale unor servicii juridice private (B12)

L

CAZUL L

Ofertă de documente ale unor servicii juridice private

Fișă de dovezi B12 | 10 nov 2026 | Forum | Servicii profesionale

Anunț neverificat

AFIRMAȚIE	Același pseudonim publică o afirmație privind documente juridice la 5 noiembrie și oferă 21.000 de documente la 10 noiembrie. Materialul pretins include documente despre clienți, proprietăți, societăți și identitate. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-11-05, 2026-11-10. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.

ALTERNATIVĂ	Un singur document poate conține mai multe persoane și contrapărți. Publicarea unei liste de nume nu demonstrează pierderi separate la fiecare organizație.
LIMITĂ	Nu sunt verificate independent fișierele, volumul sau proveniența. Contrapărțile din ofertă nu devin prin aceasta victime ale unei intruziuni.
RĂSPUNS	Examinați partajarea cu terți, verificarea identității și descărcările neobișnuite. Validați corespondența prin evidențe autorizate.
DECIZIE	Controalele relevante includ partajarea confidențială, descărcările în volum și schimbarea instrucțiunilor juridice sau de plată. Păstrați materialul sensibil prin canale aprobate.

Concluzie

Nu sunt verificate independent fișierele, volumul sau proveniența. Contrapărțile din ofertă nu devin prin aceasta victime ale unei intruziuni.

Fișă de dovezi B12 — 10 nov 2026

ternny Forum Forum EN

ORIGINAL

It is for sale 21,000 private and confidential documents

TRADUCERE

Sunt de vânzare 21.000 de documente private și confidențiale

Ce este documentat

Același pseudonim publică o afirmație privind documente juridice la 5 noiembrie și oferă 21.000 de documente la 10 noiembrie. Materialul pretins include documente despre clienți, proprietăți, societăți și identitate.

Ce nu este stabilit

Nu sunt verificate independent fișierele, volumul sau proveniența. Contrapărțile din ofertă nu devin prin aceasta victime ale unei intruziuni.

4.16 Cazul M: Ofertă de acces administrativ la o platformă comercială (B13)

CAZUL M

M

Ofertă de acces administrativ la o platformă comercială

Fișă de dovezi B13 | 10 nov 2026 | Forum | Comerț

Anunț neverificat

AFIRMAȚIE	La 10 noiembrie, un vânzător oferă acces administrativ la o platformă comercială românească, inclusiv comenzi, clienți, informații de livrare și date bancare. [S1]
CRONOLOGIE	Dosarul conține postări datate 2026-11-10. Sunt date de publicare, nu date ale intruziunii stabilite independent.
DOVEZI DEȚINUTE	Textul sursei păstrate stabilește anunțul și formularea sa. Accesul și datele oferite rămân neverificate.
ALTERNATIVĂ	O captură ori o descriere ar putea arăta acces vechi sau limitat. Afirmația despre date bancare nu stabilește expunerea numerelor de card.
LIMITĂ	Postarea păstrată nu oferă o dovadă. Accesul funcțional, copierea, confirmarea victimei, numărul persoanelor și vânzarea rămân necunoscute.
RĂSPUNS	Verificați sesiunile și privilegiile administrative, păstrați jurnalele și examinați exporturile și schimbările datelor de plată.
DECIZIE	Dovezile sesiunilor administrative sunt mai utile decât atribuirea publică imediată. Separați accesul la date, modificarea setărilor de plată și copierea confirmată.

Concluzie

Postarea păstrată nu oferă o dovadă. Accesul funcțional, copierea, confirmarea victimei, numărul persoanelor și vânzarea rămân necunoscute.

Fișă de dovezi B13 10 nov 2026

NorthDivision Forum Forum EN

ORIGINAL

Selling actual admin panel access into [retail platform]

TRADUCERE

Vând acces efectiv la panoul de administrare al [unei platforme de retail]

Ce este documentat
La 10 noiembrie, un vânzător oferă acces administrativ la o platformă comercială românească, inclusiv comenzi, clienți, informații de livrare și date bancare.

Ce nu este stabilit
Postarea păstrată nu oferă o dovadă. Accesul funcțional, copierea, confirmarea victimei, numărul persoanelor și vânzarea rămân necunoscute.

4.17 Alte oferte de servicii și limite

O ofertă din aprilie descrie acces la distanță asociat României. Nu stabilește o anumită victimă sau date de autentificare valide. În noiembrie, alt anunț oferă căutări despre vehicule la 10 USD pentru 1.000 de căutări. Niciunul nu stabilește acces neautorizat la un registru oficial. [S1]

Controlul practic pentru un serviciu comparabil este verificarea autorității pentru căutări în volum și a utilizării neobișnuite. Pentru accesul la distanță, examinați proprietatea contului, MFA, încrederea în dispozitiv și sesiunile recente. Numele unui produs în anunț nu dovedește exploatarea unei vulnerabilități a acelui produs.

Niciun anunț păstrat nu este asociat cazurilor oficiale din capitolul 5 doar pentru că sectorul sau țara sunt similare. Raportul nu trasează astfel o relație între aceste populații fără un element comun concret.

Anunțuri automate de la sfârșitul lui octombrie promovează și baze de date ale unor site-uri mici. Volumele declarate nu stabilesc originea, persoanele afectate sau intruziuni distincte confirmate. Verificați proprietatea și actualitatea prin dovezi interne autorizate înainte de escaladare. [S1]

O ofertă despre un comerciant de modă, datată 2026-01-02, promovează 84.792 de linii pentru 200 USD, dar indică o intruziune la 2026-01-29. Datele se contrazic. Textul nu clarifică cronologia, originea, accesul sau vânzarea. Păstrați contradicția fără a deduce o dată a intruziunii sau caracterul fictiv al ofertei. [S1]

O postare din octombrie pretinde și publicarea bazei de date a unui site nenominalizat. Descrierea nu stabilește conținutul, populația sau originea. Rămâne o afirmație neverificată despre publicare, nu un incident confirmat sau o populație afectată măsurată. [S1]

O relatare de monitorizare din 9 ianuarie a descris o licitație pentru acces la panoul WordPress și la shell-ul unui magazin online din România. Materialul păstrat dovedește circulația ofertei; accesul funcțional, oferta directă a vânzătorului și captura de ecran menționată rămân neverificate. [S1]

Postări din 20 septembrie și 5 octombrie au repetat afirmația că oferă un milion de înregistrări de contact mobil din România, cu câmpuri de identificare de bază. Formularea repetată susține o singură temă de date promovate. Ea nu validează numărul înregistrărilor, persoanele distincte, proveniența sau o nouă breșă la o organizație românească. [S1]

Două înregistrări de forum păstrate, datate 11 aprilie, au promovat o bază de date asociată unui site de retail românesc nenominalizat. Oferta a pretins 48.183 de rânduri, câmpuri de identificare și contact de bază și o breșă la 9 aprilie. O intrare din 26 aprilie a fost doar o readucere a firului în atenție. Înregistrările dovedesc circulația unei singure oferte; autenticitatea, proveniența, numărul persoanelor afectate și data pretinsei intruziuni rămân neverificate. [S1]

4.18 Cazul N: Ofertă de documente de identitate și liste de pasageri din aviația privată (B24)

CAZUL N

N

Ofertă de documente de identitate și liste de pasageri din aviația privată

Anunț neverificat

Fișă de dovezi B24 | 4 sep 2026 | Telegram | Transport și servicii

AFIRMAȚIE	La 4 septembrie, o postare pe o piață online a pretins că oferă documente de identitate și liste de pasageri asociate unui operator de aviație privată nenominalizat. Anunțul indica 2.600 de documente de identitate ale pasagerilor, încă 100 de pașapoarte ale membrilor de echipaj și 6.000 de fișiere, în total 2 GB. Acestea sunt numere declarate de fișiere și documente, nu persoane distincte validate. O postare din 20 septembrie a repetat o mare parte din ofertă. [S1]
CRONOLOGIE	Postările sunt datate 2026-09-04 și 2026-09-20. Nu stabilesc accesul inițial sau data obținerii documentelor.
DOVEZI DEȚINUTE	Cele două postări păstrate arată că afirmația a circulat. Formularea ulterioară nu dovedește o a doua intruziune sau o vânzare încheiată.
LIMITĂ ȘI ALTERNATIVĂ	Perioada declarată de șase ani nu datează o intruziune. Autenticitatea, valabilitatea și proveniența documentelor, precum și orice legătură cu sistemele active ale operatorului, rămân neverificate. Sunt posibile materiale mai vechi, evidențe gestionate de terți sau publicitate înșelătoare.
RĂSPUNS	Verificați proveniența și exporturile autorizate de documente înainte de a stabili persoanele afectate. Analizați evidențele de prelucrare a datelor pasagerilor și de acces al terților, apoi evaluați riscul de uzurpare a identității pentru orice grup afectat în mod real.

Concluzie

Perioada declarată de șase ani nu datează o intruziune. Autenticitatea, valabilitatea și proveniența documentelor, precum și orice legătură cu sistemele active ale operatorului, rămân neverificate. Sunt posibile materiale mai vechi, evidențe gestionate de terți sau publicitate înșelătoare.

Fișă de dovezi B24 — 4 sep 2026

Escanors Marketplace | Telegram | Telegram | EN

ORIGINAL

We have 2,600 passports/national ids/residential permits

TRADUCERE

Avem 2.600 de pașapoarte, acte naționale de identitate sau permise de ședere

Ce este documentat

O ofertă din 4 septembrie pretinde 2.600 de documente de identitate ale pasagerilor, 100 de pașapoarte ale echipajului și 6.000 de fișiere, în total 2 GB. Republicarea din 20 septembrie nu stabilește altă intruziune sau transfer încheiat.

Ce nu este stabilit

Perioada declarată de șase ani nu datează o intruziune. Autenticitatea, valabilitatea și proveniența documentelor, precum și orice legătură cu sistemele active ale operatorului, rămân neverificate. Sunt posibile materiale mai vechi, evidențe gestionate de terți sau publicitate înșelătoare.

CONCLUZII PRINCIPALE

01

Paisprezece dosare descriu afirmații din anunțuri, nu intruziuni confirmate.

02

Păstrați separat întrebările despre vechimea datelor, acces, identitatea fișierelor și vânzări.

03

Verificați sesiunile administrative, exporturile și permisiunile furnizorilor prin dovezi interne autorizate.

CAPITOLUL 05

Incidente oficiale și decizii sectoriale

05

ÎNTREBAREA ACESTUI CAPITOL

Ce comunicări oficiale schimbă răspunsul și ce întrebări rămân neclarificate?

5.1 Decizii pe sectoare 48
5.2 Cazul O: Perturbare IT la un transportator de energie 49
5.3 Cazul P: Aplicații administrative afectate de ransomware 50
5.4 Cazul Q: Indisponibilitatea unei aplicații pentru achiziții 51
5.5 Cazul R: Izolarea serviciilor după ransomware în administrația penitenciară 52
5.6 Cazul S: DNSC raportează o posibilă perturbare DDoS a site-ului 53
5.7 Cazul T: Incident la un serviciu auxiliar pentru investitori 54
5.8 Cazul U: Investigarea rețelei interne la un operator de comunicații 55
5.9 Cazul V: Lipsa MFA într-un caz de ransomware din turism 56
5.10 Cazul W: Măsuri pentru accesul la distanță și jurnalizare 57
5.11 Cazul X: Sancțiune pentru un furnizor de credit după un atac IT 58
5.12 Cazul Y: Date reale pe un server de testare 59
5.13 Cazul Z: Date administrative de autentificare obținute prin phishing 60
5.14 Cazul AA: Două deficiențe ale aplicațiilor de telecomunicații 61
5.15 Cazul AB: Accesul unui angajat bancar în afara atribuțiilor 62
5.16 Cazul AC: Prelucrarea greșită a notificărilor bancare 63
5.17 Cazul AD: DDoS asupra platformelor consulare 64
5.18 Cazul AE: Posibile interferențe cu instalații frigorifice 65
5.19 Cazul AF: Izolarea unui site fiscal pe rectorat după ransomware 66
5.20 Cazul AG: Suspendarea și reconstruirea unui portal de utilități 67
5.21 Cazul AH: Relatare privind imagini de supraveghere accesibile public 68
5.22 Cazul AI: Comunicarea din aprilie despre accesul militar anterior 69
5.23 Cazul AJ: Intervenție după un atac ransomware la o bancă din România 70
5.24 Cazul AK: Modificarea neautorizată a unui site de facultate întrerupe accesul 71
5.25 Cazul AL: Documente accesate printr-un portal de deschidere a conturilor 72
5.26 Cazul AM: Întreruperea serviciilor unei librării și redeschiderea din noiembrie 73
5.27 Cazul AN: Servicii universitare academice și administrative perturbate 74
5.28 Cazul AO: Acces restricționat la un portal guvernamental după sesizări privind datele personale 75
5.29 Cazul AP: O direcție fiscală locală a anunțat atacuri repetate 76
5.30 Cazul AQ: Site-uri ale primăriilor investigate după întreruperea accesului 77
5.31 Cazul AR: Plăți locale online indisponibile și înlocuirea planificată a sistemului 78
5.32 Cazul AS: Defigurarea repetată a unui site public din transporturi 79
5.33 Recuperarea nu clarifică toate întrebările despre dovezi 79

31

Cazul AE: Izolarea unui site fiscal pe rectorat după ransomware

Cazul AF: Detaliate bazate pe relatări oficiale, separate de ofertele clandestine

CAPITOLUL 05

Incidente oficiale și decizii sectoriale

PE SCURT

Relatările oficiale descriu perturbarea sistemelor IT de afaceri, aplicații publice indisponibile, ransomware și deficiențe în protecția datelor. Mai multe declarații păstrează explicit limite privind operațiunile sau bazele de date. Excluderile contează, dar constatările preliminare se pot schimba. Cazurile separă data incidentului de publicare și erorile interne de atacurile externe. Organizați recuperarea în jurul fluxului de afaceri, apoi desemnați responsabili separați pentru date, identitate și notificare.

5.1 Decizii pe sectoare

Sector	Dovezi	Limita interpretării	Primul responsabil
Servicii publice	Aplicații și izolarea serviciilor	Restabilirea accesului nu clarifică întreaga confidențialitate	Responsabil serviciu și coordonator incident
Energie	Perturbare IT de afaceri și constatări privind datele	Impactul IT nu stabilește acces la controlul operațional	IT și operațiuni
Servicii financiare	Aplicație auxiliară și accesul angajaților	Datele clienților și integritatea decontării cer verificări separate	Securitate, operațiuni și protecția datelor
Telecom	Incident intern și deficiențe ale aplicațiilor	Continuitatea pentru clienți nu clarifică toate întrebările despre date	Asigurarea serviciului
Tehnologie	Date personale pe un server de testare	Eticheta de testare nu elimină consecințele privind datele	Inginerie și responsabil date
Turism	Ransomware și acces la distanță	Sancțiunea recentă nu presupune un atac recent	Responsabil afaceri și infrastructură

Cazurile sunt dosare editoriale. Unele conțin o succesiune de actualizări sau mai multe constatări. Numărul lor nu reprezintă incidente naționale unice. [S20][S21][S22][S23][S24][S25][S26][S27]

5.2 Cazul O: Perturbare IT la un transportator de energie

CAZUL O

Perturbare IT la un transportator de energie

Energie

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	Compania a raportat un atac asupra sistemelor IT de afaceri și indisponibilitatea temporară a site-ului. A precizat că sistemele operaționale SCADA și telecomunicațiile nu au fost afectate, iar transportul a continuat normal. [S20]
CRONOLOGIE	Publicat la 2026-02-04. Sursa datează incidentul sau detectarea la 2026-02-03. Data nu stabilește neapărat accesul inițial.
NECLARIFICAT	Comunicarea nu stabilește accesul inițial, autorul, exfiltrarea sau familia ransomware.
TESTUL DECIZIEI	Pot funcționa finanțele și comunicarea publică în timp ce sistemele IT de afaceri sunt izolate?
RĂSPUNS	Testați recuperarea sistemelor de afaceri și izolarea de sistemele operaționale. Verificați accesul furnizorilor și administratorilor.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Comunicarea nu stabilește accesul inițial, autorul, exfiltrarea sau familia ransomware.

5.3 Cazul P: Aplicații administrative afectate de ransomware

CAZUL P

P

Aplicații administrative afectate de ransomware

Administrație publică

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	Guvernul a afirmat că ransomware a criptat și șters o parte a infrastructurii virtuale care găzduia aplicații. A precizat că baza cadastrală centrală nu a fost afectată și nu existau dovezi de acces la acele evidențe. [S21]
CRONOLOGIE	Publicat la 2026-07-27. Sursa datează incidentul sau detectarea la 2026-07-14. Data nu stabilește neapărat accesul inițial.
STATUTUL SURSEI	Copia publicată de presă este anexa preliminară DNSC din 22 iulie 2026. DNSC precizează că publicarea online nu a fost autorizată și documentul nu era raportul final. [S75][S115]
NECLARIFICAT	Anexa preliminară susține separat extragerea unui director auxiliar de conturi și deteriorarea infrastructurii virtuale. Nu susține afirmația relatată că registrul central a fost șters. Numărul total de persoane rămâne necuantificat. [S75][S76]
TESTUL DECIZIEI	O bază de referință intactă poate fi folosită când aplicațiile și serviciile de identitate sunt indisponibile?
RĂSPUNS	Restabiliți aplicațiile și dependențele de identitate într-o ordine testată. Verificați separat integritatea evidențelor de referință.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Declarația nu stabilește impactul complet asupra altor date ale utilizatorilor. Calendarul recuperării rămânea neclar. Anexa DNSC publicată de presă este preliminară; publicarea nu a fost autorizată și nu este raportul final.

5.4 Cazul Q: Indisponibilitatea unei aplicații pentru achiziții

CAZUL Q

Indisponibilitatea unei aplicații pentru achiziții

Administrație publică

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	Ministerul a anunțat un incident care afecta o aplicație de achiziții pentru beneficiari privați ai proiectelor de politică de coeziune. Aplicația nu putea fi accesată și nu era folosită pentru proiectele planului de redresare. [S22][S61]
CRONOLOGIE	Publicat la 2026-07-16. Sursa datează incidentul sau detectarea la 2026-07-15. Data nu stabilește neapărat accesul inițial.
NECLARIFICAT	Comunicarea nu stabilește furtul de date, autorul, familia malware, debutul sau accesul inițial.
TESTUL DECIZIEI	Pot beneficiarii demonstra depunerea la timp când aplicația normală este indisponibilă?
RĂSPUNS	Cartografiați termenele achizițiilor și canalele alternative de depunere. Păstrați jurnalele aplicației și identităților.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Comunicarea nu stabilește furtul de date, autorul, familia malware, debutul sau accesul inițial.

Autoritatea regională a datat ulterior întreruperea de la 15 iulie și a anunțat recuperarea la 18 august. A descris migrarea în Cloudul Guvernamental și prelungirea termenelor prin Ordinul 1143/2026. Recuperarea actualizează cazul, nu creează alt incident. [S61]

5.5 Cazul R: Izolarea serviciilor după ransomware în administrația penitenciară

R

CAZUL R

Izolarea serviciilor după ransomware în administrația penitenciară

Administrație publică

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	Instituția a raportat ransomware pe stații și servere. A suspendat unele servicii digitale și a izolat sistemele. Verificările preliminare din ziua următoare indicau că bazele importante și copiile de siguranță nu erau afectate; alte baze erau parțial afectate. [S23][S24]
CRONOLOGIE	Publicat la 2026-07-29. Sursa datează incidentul sau detectarea la 2026-07-29. Data nu stabilește neapărat accesul inițial.
NECLARIFICAT	Actualizarea următoarei zile indica o cale de intrare necunoscută. Constatările preliminare nu stabilesc sfera finală.
TESTUL DECIZIEI	Pot continua contactele esențiale fără platforma digitală normală?
RĂSPUNS	Exersați izolarea locațiilor, continuitatea contactelor esențiale și restabilirea din copii verificate independent.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Actualizarea următoarei zile indica o cale de intrare necunoscută. Constatările preliminare nu stabilesc sfera finală.

5.6 Cazul S: DNSC raportează o posibilă perturbare DDoS a site-ului

CAZUL S

S

DNSC raportează o posibilă perturbare DDoS a site-ului

Administrație publică

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	DNSC a raportat dificultăți temporare de acces și un volum neobișnuit de cereri din mai multe surse. A descris DDoS ca posibilitate și a afirmat că măsurile de protecție au stabilizat site-ul. [S25]
CRONOLOGIE	Publicat la 2026-09-08. Sursa datează incidentul sau detectarea la 2026-09-08. Data nu stabilește neapărat accesul inițial.
NECLARIFICAT	Comunicarea nu stabilește un autor sau acces în sistemele interne.
TESTUL DECIZIEI	Pot utilizatorii distinge un site indisponibil de un serviciu național de răspuns indisponibil?
RĂSPUNS	Exersați escaladarea traficului, coordonarea furnizorilor și un canal independent pentru comunicarea incidentelor.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Comunicarea nu stabilește un autor sau acces în sistemele interne.

5.7 Cazul T: Incident la un serviciu auxiliar pentru investitori

T

CAZUL T

Incident la un serviciu auxiliar pentru investitori

Servicii financiare

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	Un operator de infrastructură a pieței de capital a raportat un atac asupra unei aplicații auxiliare pentru investitori. A precizat că decontarea și registrul funcționau normal, fără acces sau modificări ale informațiilor despre deținere ori tranzacții decontate. [S26]
CRONOLOGIE	Publicat la 2026-10-16. Data atacului nu este stabilită. Dosarul este numărat după comunicare, nu ca atac nou datat.
NECLARIFICAT	Comunicarea nu indică data atacului, numărul persoanelor sau categorii detaliate de date. Data publicării nu este data atacului.
TESTUL DECIZIEI	Poate organizația verifica integritatea funcțiilor pieței în timp ce investighează separat accesul la datele investitorilor?
RĂSPUNS	Separați asistența privind identitatea investitorilor de verificarea integrității decontării. Bazați avertismentele de phishing pe date afectate validate.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Comunicarea nu indică data atacului, numărul persoanelor sau categorii detaliate de date. Data publicării nu este data atacului.

5.8 Cazul U: Investigarea rețelei interne la un operator de comunicații

CAZUL U

U

Investigarea rețelei interne la un operator de comunicații

Telecomunicații

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	Compania a raportat un incident detectat la 06:30, cu caracteristici preliminare de ransomware. A suspendat preventiv e-mailul. Compania și DNSC au precizat că serviciile clienților continuau, fără indicii atunci privind afectarea lor. [S27]
CRONOLOGIE	Publicat la 2026-10-19. Sursa datează incidentul sau detectarea la 2026-10-19. Data nu stabilește neapărat accesul inițial.
NECLARIFICAT	Impactul asupra datelor, determinarea finală a malware și accesul inițial rămâneau investigate.
TESTUL DECIZIEI	Se poate coordona personalul când e-mailul obișnuit a fost suspendat?
RĂSPUNS	Exersați comunicarea internă separată și continuitatea serviciilor clienților. Verificați recuperarea și comunicările incidentului.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Impactul asupra datelor, determinarea finală a malware și accesul inițial rămâneau investigate.

5.9 Cazul V: Lipsa MFA într-un caz de ransomware din turism

CAZUL V

V

Lipsa MFA într-un caz de ransomware din turism

Ospitalitate

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	ANSPDCP a afirmat că ransomware a exploatat o conexiune la distanță fără autentificare multifactor. Date personale ale clienților și angajaților au fost accesate neautorizat. Autoritatea a aplicat o amendă de 5.000 EUR. [S33]
CRONOLOGIE	Publicat la 2026-11-17. Data atacului nu este stabilită. Dosarul este numărat după comunicare, nu ca atac nou datat.
NECLARIFICAT	Investigația s-a încheiat în octombrie. Nu sunt precizate data atacului, numărul persoanelor sau autorul. Este o publicare recentă, nu o intruziune datată în noiembrie.
TESTUL DECIZIEI	Inventarul accesului la distanță include furnizorii și administrarea de urgență?
RĂSPUNS	Cereți MFA pentru fiecare cale de administrare la distanță și verificați jurnalele sesiunilor după modificări.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Investigația s-a încheiat în octombrie. Nu sunt precizate data atacului, numărul persoanelor sau autorul. Este o publicare recentă, nu o intruziune datată în noiembrie.

5.10 Cazul W: Măsuri pentru accesul la distanță și jurnalizare

CAZUL W

W

Măsuri pentru accesul la distanță și jurnalizare

Energie și servicii industriale

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	ANSPDCP a constatat divulgarea datelor personale și acces neautorizat după un atac IT. A aplicat o amendă de 8.000 EUR și a cerut jurnalizarea accesului și conexiuni sigure la distanță, cu VPN și MFA. [S34]
CRONOLOGIE	Publicat la 2026-11-13. Data atacului nu este stabilită. Dosarul este numărat după comunicare, nu ca atac nou datat.
NECLARIFICAT	Nu sunt precizate data atacului, autorul sau numărul persoanelor. Categoriile de date nu cuantifică indivizii afectați.
TESTUL DECIZIEI	Poate echipa reconstrui ce identitate privilegiată a accesat anumite informații?
RĂSPUNS	Verificați jurnalele accesului privilegiat, retenția și protejarea conexiunilor la distanță prin dovezi operaționale.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Nu sunt precizate data atacului, autorul sau numărul persoanelor. Categoriile de date nu cuantifică indivizii afectați.

5.11 Cazul X: Sancțiune pentru un furnizor de credit după un atac IT

CAZUL X

X

Sancțiune pentru un furnizor de credit după un atac IT

Servicii financiare

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	ANSPDCP a raportat un atac IT care afecta confidențialitatea, integritatea și securitatea datelor personale. A aplicat o amendă de 10.000 EUR după o investigație din octombrie. [S35]
CRONOLOGIE	Publicat la 2026-11-11. Data atacului nu este stabilită. Dosarul este numărat după comunicare, nu ca atac nou datat.
NECLARIFICAT	Comunicarea nu stabilește data intruziunii, familia atacului, autorul sau numărul victimelor.
TESTUL DECIZIEI	Dovezile recuperării tehnice susțin aceeași sferă a datelor folosită în comunicarea cu clienții?
RĂSPUNS	Corelați accesul la datele clienților, angajaților și partenerilor cu notificarea incidentului și dovezile recuperării testate.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Comunicarea nu stabilește data intruziunii, familia atacului, autorul sau numărul victimelor.

5.12 Cazul Y: Date reale pe un server de testare

CAZUL Y

Y

Date reale pe un server de testare

Tehnologie

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	ANSPDCP a constatat că un atac asupra unui server de testare software a expus date personale. Folosirea datelor reale a agravat impactul. Autoritatea a aplicat o amendă de 6.000 EUR și a cerut date fictive pentru testare. [S36]
CRONOLOGIE	Publicat la 2026-10-16. Data atacului nu este stabilită. Dosarul este numărat după comunicare, nu ca atac nou datat.
NECLARIFICAT	Nu sunt precizate autorul, data intruziunii sau numărul persoanelor. Mediul de testare poate avea consecințe asupra datelor de producție.
TESTUL DECIZIEI	Testarea își poate îndeplini scopul fără date reale despre clienți sau angajați?
RĂSPUNS	Înlocuiți înregistrările personale de producție din mediile de dezvoltare. Verificați izolarea și controlul accesului.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Nu sunt precizate autorul, data intruziunii sau numărul persoanelor. Mediul de testare poate avea consecințe asupra datelor de producție.

5.13 Cazul Z: Date administrative de autentificare obținute prin phishing

Z

CAZUL Z

Date administrative de autentificare obținute prin phishing

Servicii pentru întreprinderi

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	ANSPDCP a constatat că phishingul a obținut datele unui utilizator cu drepturi administrative. Datele personale ale clienților au fost accesate neautorizat. Autoritatea a aplicat o amendă de 3.000 EUR. [S37]
CRONOLOGIE	Publicat la 2026-08-19. Data atacului nu este stabilită. Dosarul este numărat după comunicare, nu ca atac nou datat.
NECLARIFICAT	Comunicarea nu cuantifică clienții și nu datează intruziunea. O identitate privilegiată nu stabilește afectarea fiecărui cont.
TESTUL DECIZIEI	Pot echipele revoca sesiunile active și accesul delegat, pe lângă resetarea parolei?
RĂSPUNS	Examinați sesiunile privilegiate și recuperarea conturilor. Exersați revocarea atât a datelor de autentificare, cât și a sesiunilor active.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Comunicarea nu cuantifică clienții și nu datează intruziunea. O identitate privilegiată nu stabilește afectarea fiecărui cont.

5.14 Cazul AA: Două deficiențe ale aplicațiilor de telecomunicații

CAZUL AA

AA

Două deficiențe ale aplicațiilor de telecomunicații

Telecomunicații

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	ANSPDCP a descris o eroare de sincronizare care expunea facturile altor clienți și un atac separat asupra unei platforme de solicitări de asistență. A aplicat două amenzi în valoare totală de 100.000 EUR. [S38]
CRONOLOGIE	Publicat la 2026-07-17. Data atacului nu este stabilită. Dosarul este numărat după comunicare, nu ca atac nou datat.
NECLARIFICAT	Comunicarea nu datează un atac nou în 2026 asupra platformei de asistență. Eroarea de facturare și atacul extern au cauze diferite.
TESTUL DECIZIEI	O autentificare legitimă rămâne limitată la propriile înregistrări în fiecare aplicație conectată?
RĂSPUNS	Testați autorizarea între aplicațiile conectate. Protejați administrarea platformei de asistență prin acces restricționat și multifactor.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Comunicarea nu datează un atac nou în 2026 asupra platformei de asistență. Eroarea de facturare și atacul extern au cauze diferite.

5.15 Cazul AB: Accesul unui angajat bancar în afara atribuțiilor

CAZUL AB

AB

Accesul unui angajat bancar în afara atribuțiilor

Servicii bancare

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	ANSPDCP a constatat că un angajat a accesat fără autorizare extrasele unor conturi de clienți, la cererea unui terț. A aplicat o amendă de 5.000 EUR și a cerut măsuri împotriva accesului în scop personal. [S40]
CRONOLOGIE	Publicat la 2026-07-02. Data atacului nu este stabilită. Dosarul este numărat după comunicare, nu ca atac nou datat.
NECLARIFICAT	Comunicarea nu stabilește un atac extern sau o prevalență sectorială.
TESTUL DECIZIEI	Poate investigatorul distinge asistența legitimă de curiozitate sau solicitările unui terț?
RĂSPUNS	Examinați accesul excepțional al angajaților, dovada scopului profesional și consultarea neexplicată a înregistrărilor clienților.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Comunicarea nu stabilește un atac extern sau o prevalență sectorială.

5.16 Cazul AC: Prelucrarea greșită a notificărilor bancare

CAZUL AC

AC

Prelucrarea greșită a notificărilor bancare

Servicii bancare

Relatare oficială: limitele precizate

RELATARE OFICIALĂ	ANSPDCP a constatat că prelucrarea manuală a unui fișier a trimis notificări de reînnoire a asigurării către destinatari greșiți. A aplicat 10.000 EUR pentru deficiențe de securitate și 2.000 EUR pentru notificarea întârziată. [S39]
CRONOLOGIE	Publicat la 2026-05-29. Data atacului nu este stabilită. Dosarul este numărat după comunicare, nu ca atac nou datat.
NECLARIFICAT	Decizia nu descrie hacking extern și nu cuantifică persoanele. Consemnează explicit depășirea termenului de 72 de ore.
TESTUL DECIZIEI	Poate echipa detecta un destinatar greșit și începe prompt evaluarea privind datele personale?
RĂSPUNS	Testați asocierea destinatarilor înainte de trimiterea în volum. Consemnați momentul de la care curg termenele de notificare.
DOVADA FINALIZĂRII	Consemnați responsabilul serviciului și al datelor, verificarea efectuată, incertitudinile și decizia. Închideți exercițiul doar când responsabilul acceptă dovezile.

Concluzie

Decizia nu descrie hacking extern și nu cuantifică persoanele. Consemnează explicit depășirea termenului de 72 de ore.

5.17 Cazul AD: DDoS asupra platformelor consulare

AD

CAZUL AD

DDoS asupra platformelor consulare

Administrație publică

Relatare cu limitele sursei

RELATAREA SURSEI	Ministerul a precizat că DDoS a încetinit două platforme pentru cetățeni și a produs întreruperi scurte. A afirmat că toate sistemele digitale au revenit la normal și informațiile sensibile nu au fost accesate. [S62]
CRONOLOGIE	Publicat la 2026-03-14. Sursa datează incidentul sau observațiile la 2026-03-13/14.
NECLARIFICAT	Nu sunt stabilite durata exactă, autorul sau volumul traficului.
TESTUL DECIZIEI	Pot cetățenii utiliza un canal alternativ când platforma publică este indisponibilă?
RĂSPUNS	Exersați continuitatea DDoS și comunicarea alternativă cu cetățenii. Separați disponibilitatea de afirmațiile despre intruziune.

Concluzie

Nu sunt stabilite durata exactă, autorul sau volumul traficului.

5.18 Cazul AE: Posibile interferențe cu instalații frigorifice

CAZUL AE

AE

Posibile interferențe cu instalații frigorifice

Comerț cu amănuntul și distribuție alimentară

Relatare cu limitele sursei

RELATAREA SURSEI	Șase magazine ale unui lanț nenumit au raportat temperaturi frigorifice anormale. DNSC a tratat relatările drept posibile incidente cibernetice, în contextul unui val european. [S63][S81]
CRONOLOGIE	Publicat la 2026-11-03. Sursa datează incidentul sau observațiile la 2026-11-02.
NECLARIFICAT	Mecanismul cibernetic din magazinele românești, pierderile, autorul și identitatea comerciantului nu sunt stabilite. Șase magazine nu înseamnă șase atacuri confirmate.
TESTUL DECIZIEI	Pot operațiunile distinge o eroare de configurare de modificări neautorizate, păstrând controlul sigur?
RĂSPUNS	Eliminați accesul direct din internet la administrare, securizați furnizorii și verificați firmware-ul, temperaturile, programele de dezgheț și alarmele.

Concluzie

Mecanismul cibernetic din magazinele românești, pierderile, autorul și identitatea comerciantului nu sunt stabilite. Șase magazine nu înseamnă șase atacuri confirmate.

5.19 Cazul AF: Izolarea unui site fiscal municipal după malware

CAZUL AF

AF

Izolarea unui site fiscal municipal după malware

Administrație publică

Relatare cu limitele sursei

RELATAREA SURSEI	Presa națională citează municipalitatea afirmând că un troian a afectat serverul site-ului fiscal. Serverul a fost deconectat, iar specialiștii investigau și restabileau serviciul. [S64]
CRONOLOGIE	Publicat la 2026-07-20. Sursa datează incidentul sau observațiile la 2026-07-20.
NECLARIFICAT	Postarea oficială inițială, impactul mai larg, accesul la date, autorul și data recuperării nu sunt stabilite din sursa citită.
TESTUL DECIZIEI	Are echipa o dovadă datată a recuperării, dincolo de anunțul izolării?
RĂSPUNS	Documentați izolarea și recuperarea sigură. Testați continuitatea serviciului pentru cetățeni și investigați căile de acces.

Concluzie

Postarea oficială inițială, impactul mai larg, accesul la date, autorul și data recuperării nu sunt stabilite din sursa citită.

5.20 Cazul AG: Suspendarea și reconstruirea unui portal de utilități

AG

CAZUL AG

Suspendarea și reconstruirea unui portal de utilități

Utilități și servicii de mediu

Relatare cu limitele sursei

RELATAREA SURSEI	Compania confirmă un incident de securitate la 7 octombrie și posibil acces neautorizat la datele clienților. A suspendat portalul și invalidat parolele, apoi a restabilit accesul la 2 noiembrie după reconstrucție, remedieri și audit extern. Serviciile de colectare au continuat. [S65][S66]
CRONOLOGIE	Publicat la 2026-11-02. Sursa datează incidentul sau observațiile la 2026-10-07.
NECLARIFICAT	Copierea datelor, numărul exact de conturi, autorul și accesul inițial rămân investigate. Comunicarea inițială nu are dată explicită de publicare; 2 noiembrie este actualizarea datată de recuperare.
TESTUL DECIZIEI	Poate fi acceptată recuperarea în timp ce investigarea copierii rămâne deschisă?
RĂSPUNS	Revocați autentificările vechi, testați serviciul reconstruit, comunicați prin canale verificate și urmăriți fraudele ulterioare.

Concluzie

Copierea datelor, numărul exact de conturi, autorul și accesul inițial rămân investigate. Comunicarea inițială nu are dată explicită de publicare; 2 noiembrie este actualizarea datată de recuperare.

5.21 Cazul AH: Relatare privind imagini de supraveghere accesibile public

CAZUL AH

AH

Relatare privind imagini de supraveghere accesibile public

Administrație publică și educație

Relatare cu limitele sursei

RELATAREA SURSEI	Reporterii au găsit imagini municipale indexate fără autentificare în septembrie–octombrie. Municipalitatea le-a comunicat suspendarea accesului extern, resetarea parolelor, actualizarea și închiderea porturilor, contestând afectarea datelor personale. Separat, autoritatea de îngrijire a copiilor a afirmat că imaginea nu stabilește proveniența ori încălcarea și a anunțat verificări. [S68][S69]
CRONOLOGIE	Publicat la 2026-11-09. Observațiile municipale sunt din septembrie–octombrie; răspunsul separat privind îngrijirea copiilor este datat 2026-11-02. Datele nu stabilesc debutul intruziunii.
NECLARIFICAT	Durata expunerii, accesul altora și proveniența exactă a imaginilor de îngrijire rămân neclarificate. Nu este stabilit un autor sau un stat responsabil.
TESTUL DECIZIEI	Pot administratorii demonstra autentificarea efectivă și justifica permisiunile de vizualizare externă?
RĂSPUNS	Inventariați camerele, restricționați accesul extern, verificați autentificarea și retenția, examinați jurnalele și documentați decizia de notificare.

Concluzie

Durata expunerii, accesul altora și proveniența exactă a imaginilor de îngrijire rămân neclarificate. Nu este stabilit un autor sau un stat responsabil.

5.22 Cazul AI: Comunicarea din aprilie despre accesul militar anterior

AI

CAZUL AI

Comunicarea din aprilie despre accesul militar anterior

E-mail în apărare

Incident anterior: comunicare în aprilie

RELATAREA SURSEI	Reuters a raportat cel puțin 67 de conturi militare afectate. Răspunsul oficial, citat de radioul național, a descris zeci de conturi accesate și 30 de încercări nereușite. A precizat detectarea în martie 2025 și izolarea în 24 de ore. [S73] [S74]
CRONOLOGIE	Comunicarea este datată 2026-04-15. Răspunsul datează detectarea în martie 2025 și descrie centralizarea responsabilității cibernetice în martie 2026. Intervalul campaniei regionale nu stabilește o intruziune românească nouă în 2026.
LIMITĂ	Răspunsul a precizat că mesajele conțineau informații administrative neclasificate sau publice. Relatarea Reuters consemnează dezacordul privind atribuirea specifică Fancy Bear. Nu există dovezi care leagă această comunicare de cazul separat Turla.
RĂSPUNS	Tratați e-mailul administrativ ca relevant pentru colectarea de informații. Verificați accesul, impuneți MFA și revocați sesiunile relevante când utilizarea neautorizată este confirmată. Păstrați clasificarea din răspunsul oficial fără a echivala neclasificat cu lipsa consecințelor.

Concluzie

Detectare în martie 2025; atribuire disputată

5.23 Cazul AJ: Intervenție după un atac ransomware la o bancă din România

CAZUL AJ

AJ

Intervenție după un atac ransomware la o bancă din România

Servicii bancare și financiare

Relatare oficială citată

RELATAREA SURSEI	DNSC a declarat că a fost notificat pe 2 august despre un atac ransomware la bancă și că, la cererea acesteia, sprijină limitarea efectelor și investigația. [S77][S78]
CRONOLOGIE	Publicat la 2026-08-04. Data atacului nu este stabilită. Data notificării este 2026-08-02. Datele nu stabilesc accesul inițial.
LIMITĂ	Comunicatul nu stabilește sistemele afectate, furtul datelor clienților, impactul asupra serviciilor, răscumpărarea sau autorul. O revendicare ulterioară rămâne separată; data ei nu înlocuiește data notificării oficiale.
RĂSPUNS	Testați refacerea serviciilor bancare, protejați accesul privilegiat și pregătiți notificările către autoritatea de supraveghere și clienți pe baza dovezilor.

Concluzie

Comunicatul nu stabilește sistemele afectate, furtul datelor clienților, impactul asupra serviciilor, răscumpărarea sau autorul. O revendicare ulterioară rămâne separată; data ei nu înlocuiește data notificării oficiale.

5.24 Cazul AK: Modificarea neautorizată a unui site de facultate întrerupe accesul

CAZUL AK

AK

Modificarea neautorizată a unui site de facultate întrerupe accesul

Educație

Relatare oficială citată

RELATAREA SURSEI	Decanul a confirmat afectarea interfeței publice a site-ului. Site-ul a fost deconectat pentru analiza jurnalelor și eliminarea fișierelor infectate, iar un audit tehnic urma să stabilească impactul. [S79]
CRONOLOGIE	Publicat la 2026-02-13. Sursa datează incidentul sau detectarea la 2026-02-13. Datele nu stabilesc accesul inițial.
LIMITĂ	Articolul descrie un mesaj de defacement, însă constatarea oficială citată este preliminară. Nu stabilește furtul datelor studenților și nu confirmă independent semnătura autorului sau metoda exactă de acces.
RĂSPUNS	Izolați serviciile web afectate, păstrați jurnalele, verificați accesul administrativ și validați instalarea curată înainte de redeschidere.

Concluzie

Articolul descrie un mesaj de defacement, însă constatarea oficială citată este preliminară. Nu stabilește furtul datelor studenților și nu confirmă independent semnătura autorului sau metoda exactă de acces.

5.25 Cazul AL: Documente accesate printr-un portal de deschidere a conturilor

CAZUL AL

AL

Documente accesate printr-un portal de deschidere a conturilor

Servicii bancare și financiare

Relatare oficială citată

RELATAREA SURSEI	Actualizarea firmei de servicii de investiții din 20 noiembrie a confirmat accesul neautorizat la serverul portalului de deschidere a conturilor, cu acces la baza de date și documente. Sistemele de monitorizare au detectat incidentul, iar serverul a fost izolat. [S80][S96]
CRONOLOGIE	Publicat la 2026-11-20. Sursa datează incidentul sau detectarea la 2026-10-30. Datele nu stabilesc accesul inițial.
LIMITĂ	Firma a declarat că incidentul a rămas în cadrul aplicației și că activele clienților au fost protejate. Numărul persoanelor afectate, datele copiate și metoda de acces nu sunt stabilite; evaluarea impactului și informarea continuau.
RĂSPUNS	Separați înrolarea clienților de tranzacționare și custodie, verificați jurnalele accesării documentelor și finalizați notificările în funcție de risc.

Concluzie

Firma a declarat că incidentul a rămas în cadrul aplicației și că activele clienților au fost protejate. Numărul persoanelor afectate, datele copiate și metoda de acces nu sunt stabilite; evaluarea impactului și informarea continuau.

5.26 Cazul AM: Întreruperea serviciilor unei librării și redeschiderea din noiembrie

AM

CAZUL AM

Întreruperea serviciilor unei librării și redeschiderea din noiembrie

Comerț și grupuri

Relatare oficială citată

RELATAREA SURSEI	Notificarea librăriei arată că un incident semnalat pe 22 octombrie a perturbat serviciile. Compania a izolat sisteme, a notificat autoritățile și a apelat la specialiști externi. Au fost afectate cumpărăturile online, fidelitatea, facturarea și voucherele. Un e-mail al companiei, relatat de Mobilissimo, a confirmat redeschiderea magazinului online pe 18 noiembrie. [S82][S83]
CRONOLOGIE	Publicat la 2026-10-29. Sursa datează incidentul sau detectarea la 2026-10-22. Datele nu stabilesc accesul inițial.
LIMITĂ	Notificarea inițială preciza că nu existau indicii de accesare sau extragere a datelor clienților, iar investigația continua. Mesajul de redeschidere nu stabilește refacerea tuturor serviciilor sau concluziile finale ale investigației.
RĂSPUNS	Testați dependențele dintre vânzări online, facturare, fidelitate și carduri cadou; comunicați refacerea fiecărui serviciu și schimbați parolele reutilizate.

Concluzie

Notificarea inițială preciza că nu existau indicii de accesare sau extragere a datelor clienților, iar investigația continua. Mesajul de redeschidere nu stabilește refacerea tuturor serviciilor sau concluziile finale ale investigației.

5.27 Cazul AN: Servicii universitare academice și administrative perturbate

CAZUL AN

AN

Servicii universitare academice și administrative perturbate

Educație și cercetare

Relatare oficială citată

RELATAREA SURSEI	Conducerea universității a anunțat un incident cibernetic care a afectat infrastructura IT și serviciile digitale folosite în activitatea academică și administrativă. A precizat că DNSC, ANSPDCP și DIICOT au fost notificate, iar specialiștii lucrau la reluarea treptată a serviciilor. [S84][S97]
CRONOLOGIE	Relatarea națională a fost publicată la 2026-07-29, după comunicarea conducerii și relatarea locală din 2026-07-28. Data atacului nu este stabilită. Datele nu stabilesc accesul inițial.
LIMITĂ	Comunicatul nu identifică autorul, nu stabilește ransomware-ul, nu cuantifică furtul de date și nu precizează data accesului inițial. Volumul și numele Qilin dintr-o revendicare rămân afirmații separate.
RĂSPUNS	Separați sistemele academice, administrative și de identitate; exersați refacerea treptată și păstrați probele pentru autoritățile notificate.

Concluzie

Comunicatul nu identifică autorul, nu stabilește ransomware-ul, nu cuantifică furtul de date și nu precizează data accesului inițial. Volumul și numele Qilin dintr-o revendicare rămân afirmații separate.

5.28 Cazul AO: Acces restricționat la un portal guvernamental după sesizări privind datele personale

AO

CAZUL AO

Acces restricționat la un portal guvernamental după sesizări privind datele personale

Guvern și administrație publică

Relatare oficială citată

RELATAREA SURSEI	După sesizări privind publicarea unor identificatori personali și adrese de domiciliu, Guvernul a declarat că a dispus o nouă verificare a documentelor, restricționarea accesului unde era necesar și revizuirea procesului de preluare și publicare. [S85]
CRONOLOGIE	Publicat la 2026-09-25. Sursa datează incidentul sau detectarea la 2026-09-25. Datele nu stabilesc accesul inițial.
LIMITĂ	Este o problemă de publicare și protecție a datelor; răspunsul nu stabilește o intruziune externă, o decizie GDPR sau numărul persoanelor afectate. Dimensiunea platformei nu reprezintă numărul persoanelor afectate.
RĂSPUNS	Verificați anonimizarea documentelor și aprobarea publicării, eliminați identificatorii excesivi și controlați accesul la fișierele deja publicate.

Concluzie

Este o problemă de publicare și protecție a datelor; răspunsul nu stabilește o intruziune externă, o decizie GDPR sau numărul persoanelor afectate. Dimensiunea platformei nu reprezintă numărul persoanelor afectate.

5.29 Cazul AP: O direcție fiscală locală a anunțat atacuri repetate

AP

CAZUL AP

O direcție fiscală locală a anunțat atacuri repetate

Guvern și administrație publică

Relatare oficială citată

RELATAREA SURSEI	Directoarea a declarat în ședința consiliului local din 29 octombrie că un atac a avut loc pe 27 august și s-a repetat zilnic timp de o săptămână. A spus că autoritățile au fost informate și a solicitat protecție antivirus și firewall mai puternică. [S87]
CRONOLOGIE	Publicat la 2026-10-30. Sursa datează incidentul sau detectarea la 2026-08-27. Datele nu stabilesc accesul inițial.
LIMITĂ	Declarația nu stabilește metoda de acces, accesarea datelor, autorul, răscumpărarea sau pierderile. Solicitarea protejării bazei de date nu dovedește accesarea ei.
RĂSPUNS	Verificați jurnalele evenimentelor repetate, separați serviciile fiscale publice de administrarea bazei de date și validați măsurile introduse.

Concluzie

Declarația nu stabilește metoda de acces, accesarea datelor, autorul, răscumpărarea sau pierderile. Solicitarea protejării bazei de date nu dovedește accesarea ei.

5.30 Cazul AQ: Site-uri ale primăriilor investigate după întreruperea accesului

AQ

CAZUL AQ

Site-uri ale primăriilor investigate după întreruperea accesului

Guvern și administrație publică

Relatare oficială citată

RELATAREA SURSEI	Poliția a anunțat verificări preliminare după relatări că mai multe site-uri ale primăriilor deveniseră indisponibile. Comunicatul descria un posibil atac cibernetic și preciza că instituțiile nu depuseseră încă sesizări oficiale. [S88]
CRONOLOGIE	Publicat la 2026-07-10. Data atacului nu este stabilită. Datele nu stabilesc accesul inițial.
LIMITĂ	Cauza, autorul, mecanismul tehnic și impactul asupra datelor nu erau stabilite. Indisponibilitatea și investigația nu confirmă o intruziune sau ransomware.
RĂSPUNS	Corelați jurnalele furnizorului de găzduire și comunicarea întreruperii înainte de a atribui o cauză.

Concluzie

Cauza, autorul, mecanismul tehnic și impactul asupra datelor nu erau stabilite. Indisponibilitatea și investigația nu confirmă o intruziune sau ransomware.

5.31 Cazul AR: Plăți locale online indisponibile și înlocuirea planificată a sistemului

CAZUL AR

AR

Plăți locale online indisponibile și înlocuirea planificată a sistemului

Guvern și administrație publică

Relatare oficială citată

RELATAREA SURSEI	Primăria a anunțat indisponibilitatea plăților online după un incident cibernetic raportat internațional care afecta platforma. Pe 16 noiembrie a anunțat un sistem înlocuitor planificat pentru 23 noiembrie, cu două zile de testare. [S89] [S90]
CRONOLOGIE	Publicat la 2026-10-22. Sursa datează incidentul sau detectarea la 2026-10-22. Datele nu stabilesc accesul inițial.
LIMITĂ	Nu sunt stabilite o intruziune locală, malware, un CVE exploatat sau pierderea datelor. Notificarea din noiembrie menționează și o problemă de acces la platforma națională; alternativa din octombrie nu trebuie prezentată ca permanent disponibilă. Lansarea planificată pe 23 noiembrie este după data-limită, nu o refacere observată.
RĂSPUNS	Testați alternativele locale și naționale de plată, publicați starea exactă a serviciilor și validați accesul înaintea redeschiderii.

Concluzie

Nu sunt stabilite o intruziune locală, malware, un CVE exploatat sau pierderea datelor. Notificarea din noiembrie menționează și o problemă de acces la platforma națională; alternativa din octombrie nu trebuie prezentată ca permanent disponibilă. Lansarea planificată pe 23 noiembrie este după data-limită, nu o refacere observată.

5.32 Cazul AS: Defigurarea repetată a unui site public din transporturi

AS

CAZUL AS

Defigurarea repetată a unui site public din transporturi

Guvern și administrație publică

Relatare oficială citată

RELATAREA SURSEI	Directorul a confirmat al doilea atac asupra site-ului în două săptămâni, a precizat că ambele au fost raportate DNSC și a descris colaborarea cu un furnizor de servicii IT pentru refacerea accesului. Site-ul afișa un mesaj de defigurare. [S98]
CRONOLOGIE	Publicat la 2026-07-03. Sursa datează incidentul sau detectarea la 2026-07-03. Datele nu stabilesc accesul inițial.
LIMITĂ	Directorul a declarat că bazele de date nu au fost afectate, iar rapoartele aveau copii și un alt depozit public. Refacerea în trei-patru ore era o estimare, nu o finalizare observată. Un pseudonim afișat nu identifică autorul și nu dovedește afectarea operațiunilor de transport.
RĂSPUNS	Închideți calea de acces repetat, păstrați jurnalele web și asigurați un depozit independent pentru rapoartele publice.

Concluzie

Directorul a declarat că bazele de date nu au fost afectate, iar rapoartele aveau copii și un alt depozit public. Refacerea în trei-patru ore era o estimare, nu o finalizare observată. Un pseudonim afișat nu identifică autorul și nu dovedește afectarea operațiunilor de transport.

5.33 Recuperarea nu clarifică toate întrebările despre dovezi

Cazurile separă sistemele IT de afaceri, aplicațiile publice, rețelele interne, evidențele de referință și sistemele operaționale. Sunt suprafețe distincte. Păstrați exact declarația că una a continuat să funcționeze, fără a o transforma în afirmația că alte date nu au fost afectate.

Nici o constatare oficială nu autentifică un anunț comercial fără legătură demonstrată. Un document autentic poate avea mai mulți deținători legitimi. Sectorul similar și datele apropiate nu stabilesc un incident sau operator comun.

Responsabilul serviciului trebuie să accepte recuperarea. Responsabilul identității decide limitarea conturilor și sesiunilor. Responsabilul datelor și echipa de protecție a datelor stabilesc evidențele afectate și notificarea. Închiderea de către o echipă nu clarifică automat întrebările celorlalte.

CONCLUZII PRINCIPALE

01

Păstrați fiecare excludere oficială în limitele și la data sa.

02

O aplicație recuperată poate lăsa deschise întrebări privind accesul și notificarea.

03

Stabiliți dovezi separate de finalizare pentru restabilire, limitarea identității și deciziile privind datele personale.

CAPITOLUL 06

Hactivism, DDoS și activitate recentă

ÎNTREBAREA ACESTUI CAPITOL

Ce separă o afirmație despre disponibilitate de impactul stabilit și ce a devenit vizibil între 8–22 noiembrie?

8–22 noiembrie

activitate recentă în intervalul complet al raportului

6.1 Disponibilitatea și accesul răspund unor întrebări diferite 82
6.2 Afirmațiile păstrate, în propriile cuvinte 82
6.3 Afirmație și relatare oficială 86
6.4 Cronologia comunicărilor și afirmațiilor 87
6.5 Activitate recentă: 8–22 noiembrie 89
6.6 Comunicarea faptului stabilit 90

CAPITOLUL 06

Hactivism, DDoS și activitate recentă

PE SCURT

Relatările oficiale disting întreruperile scurte ale serviciilor publice și posibilul DDoS de intruziune sau acces la date. Perioada finală a adus două oferte de forum relevante, relatări despre spionaj, decizii privind datele și avertismente de fraudă. Mai multe publicări recente privesc evenimente vechi. Verificați impactul prin dovezi operaționale, păstrați cronologia inițială și pregătiți o cale independentă de comunicare înaintea următoarei afirmații.

6.1 Disponibilitatea și accesul răspund unor întrebări diferite

Ministerul de Externe a raportat încetiniri și întreruperi scurte legate de DDoS, care au afectat două platforme pentru cetățeni la 13–14 martie. A precizat că serviciile au revenit la normal și informațiile sensibile nu au fost accesate. Declarația nu stabilește autorul sau volumul traficului. [S62]

La 8 septembrie, DNSC a descris dificultăți temporare de acces la site și un număr neobișnuit de cereri din mai multe surse. A considerat DDoS o posibilitate și a afirmat că protecțiile au stabilizat site-ul. Aceasta nu stabilește o intruziune internă sau o grupare responsabilă. [S25]

Relatările susțin planificarea continuității pentru servicii concrete. Nu validează fiecare afirmație cu mesaj politic și nu leagă cele două evenimente. O captură a unei pagini indisponibile poate surprinde un moment fără a stabili durata, cauza sau impactul de afaceri.

6.2 Afirmațiile păstrate, în propriile cuvinte

La 11 martie, 313 Team a publicat afirmații despre site-uri de servicii publice. Un fragment arab spune că atacul va continua două ore. Este o formulare prospectivă, nu măsurarea unei întreruperi încheiate. Nu este asociată relatării ministerului despre 13–14 martie. [S1][S62]

Fișă de dovezi B14 — 11 mar 2026

313 Team | Telegram | Telegram | AR

ORIGINAL

سيستمر الهجوم لساعتين.

TRADUCERE

Atacul va continua timp de două ore.

Ce este documentat
Contul a indicat o durată pentru o afirmație despre un site de servicii publice.

Ce nu este stabilit
Durata și impactul nu au fost măsurate independent. Formularea arabă privește viitorul.

Postări DDoSia Project cu semnătura NoName057(16) au descris ținte românești în 16–21 martie. Au numit servicii publice, transport, energie și finanțe. Postări ulterioare din vară au repetat afirmații de vizare a României. Listele și legăturile de disponibilitate nu stabilesc perturbare susținută ori acces intern. [S1]

Fișă de dovezi B15 — 17 mar 2026

DDoSia Project | Telegram | Telegram | RU

ORIGINAL

Продолжаем [...] атаковать Румынию

TRADUCERE

Continuăm [...] să atacăm România.

Ce este documentat
O postare din martie enumeră ținte de servicii publice și poartă semnătura NoName057(16).

Ce nu este stabilit
Nu sunt stabilite independent întreruperea, impactul de afaceri sau identitatea operatorului.

Fișă de dovezi B19 — 1 aug 2026

NoName-labelled account | Telegram | Telegram | EN

ORIGINAL

Continuing our "tour" of Romania

TRADUCERE

Ne continuăm „turul" prin România

Ce este documentat
O postare din august enumeră mai multe site-uri românești de servicii publice drept ținte.

Ce nu este stabilit
Lista nu stabilește indisponibilitate susținută sau impact asupra serviciilor interne.

Afirmația BD Anonymous din 28 iulie privește un site cu temă de servicii publice. Nu stabilește o întrerupere măsurată independent. [S1]

Fișă de dovezi B18 — 28 iul 2026

BD Anonymous | Telegram | Telegram | EN

ORIGINAL

We have successfully took down

TRADUCERE

Am scos din funcțiune cu succes

Ce este documentat
Contul a pretins perturbarea unui site cu temă de servicii publice.

Ce nu este stabilit
Citatul reprezintă formularea autorului. Nu este stabilită independent o întrerupere.

O relatare etichetată ServerKillers din 12 septembrie indică durata pretinsă a perturbării unor site-uri de servicii publice. Durata rămâne o afirmație retransmisă; nu sunt stabilite un operator comun sau o întrerupere măsurată. [S1]

Fișă de dovezi B20 — 12 sep 2026

ServerKillers-labelled relay | Telegram | Telegram | EN

ORIGINAL

Duration: 5 hours.

TRADUCERE

Durată: 5 ore.

Ce este documentat
O relatare din septembrie indică o durată pentru pretinse perturbări ale unor site-uri de servicii publice.

Ce nu este stabilit
Durata este o afirmație preluată; nu sunt stabilite un operator comun sau o întrerupere măsurată.

Alte afirmații privesc interfața unei spălătorii, accesul la supraveghere și un panou administrativ din aprilie. Limba, captura și declarația de acces nu stabilesc proprietarul, locația, controlul sau efecte fizice. Niciuna nu este legată de posibilele incidente frigorifice din noiembrie. [S1][S63]

Fișă de dovezi B16 — 17 mar 2026

DDoSia Project | Telegram | Telegram | EN

ORIGINAL

The interface is entirely in Romanian.

TRADUCERE

Interfața este integral în limba română.

Ce este documentat
Postarea descrie presupus acces la o interfață de control a unei spălătorii auto.

Ce nu este stabilit
Limba interfeței nu stabilește locația, controlul funcțional sau efecte fizice.

Fișă de dovezi B17 — 30 oct 2026

RBL Leviathan Ghost | Telegram | Telegram | EN

ORIGINAL

Team1914 | Romania CCTV Access

TRADUCERE

Team1914 | Acces CCTV în România

Ce este documentat
Postarea conține o afirmație etichetată Team1914 despre acces la supraveghere în România.

Ce nu este stabilit
Nu sunt validate dispozitivul, sesiunea, proprietarul sau relația dintre operatori.

Fișă de dovezi B21 — 7 apr 2026

Access-claim account | Telegram | Telegram | RU

ORIGINAL

Был получен полный доступ к системе

TRADUCERE

A fost obținut acces complet la sistem.

Ce este documentat
O postare din aprilie pretinde acces administrativ la o platformă de servicii din România.

Ce nu este stabilit
Formularea este afirmația autorului. Nu sunt validate accesul, arhiva sau transferul ulterior.

Unele retransmiteri din august, pe un cont etichetat NoName, poartă semnături Darkstorm. Acestea stabilesc retransmiterea unei afirmații, nu un operator comun sau o alianță formală. Materialul nu oferă o măsurare independentă a perturbării susținute a serviciilor românești. [S1]

Postări datate 30 și 31 iulie pretind și acces la interfețe de control din producție. Etichetele despre rețete, temperaturi și forță nu stabilesc proprietatea, controlul funcțional sau efecte asupra producției. Afirmațiile nu sunt legate de relatările ulterioare despre refrigerare. Verificați accesul administrativ și dovezile procesului fizic împreună cu responsabilul echipamentului. [S1]

Fișă de dovezi B22	30 iul 2026

NoName-labelled account | Telegram | Telegram | EN

ORIGINAL

Recipes. Vacuum. Temperatures. Cycle management.

TRADUCERE

Rețete. Vid. Temperaturi. Gestionarea ciclului.

Ce este documentat
O postare din 30 iulie descrie acces pretins la o interfață de control din producție.

Ce nu este stabilit
Nu sunt validate independent accesul funcțional, proprietatea sau locația echipamentelor, modificarea comenzilor ori efecte asupra producției.

Fișă de dovezi B23	31 iul 2026

NoName-labelled account | Telegram | Telegram | EN

ORIGINAL

Recipes, temperatures, closing force

TRADUCERE

Rețete, temperaturi, forță de închidere

Ce este documentat
O postare din 31 iulie descrie acces pretins la o altă interfață de control din producție.

Ce nu este stabilit
Nu sunt validate independent accesul funcțional, proprietatea sau locația echipamentelor, modificarea comenzilor ori efecte asupra producției.

Afirmațiile din vară au enumerat în mod repetat site-uri de logistică și servicii maritime, inclusiv pagini de rezervare și autentificare. Ele descriu presupuse întreruperi ale serviciilor web: o listă de ținte nu dovedește accesul la sistemele de marfă, întreruperea operațiunilor portuare sau modificarea tranzacțiilor. [S1]

La 17 septembrie, o relatare etichetată ServerKillers a susținut că un site public din sectorul financiar românesc a fost indisponibil timp de trei ore. Nu există în materialul păstrat o măsurare independentă a întreruperii. Afirmația nu dovedește accesul la sisteme financiare, întreruperea tranzacțiilor sau expunerea datelor clienților. [S1]

6.3 Afirmație și relatare oficială

Panoul păstrează întrebările separate. Este un instrument pentru decizii, nu reconcilierea unor măsurători incompatibile.

Întrebare	Afirmație infracțională sau publică	Relatare oficială ori a sursei	Limita deciziei
Poate fi folosit un cont administrativ?	Ofertă din noiembrie privind accesul la o platformă comercială [S1]	Nu este stabilită o confirmare corespondentă în dovezile citate	Verificați sesiunile; nu autentificați afirmația vânzătorului
A fost perturbat un serviciu public?	O întrerupere poate fi amplificată ca afirmație de atac	Ministerul descrie întreruperi scurte în martie și restabilirea serviciului [S62]	Păstrați limitele precizate de minister
A fost accesată rețeaua internă DNSC?	Dificultatea site-ului public poate fi prezentată ca impact mai larg	DNSC descrie dificultatea site-ului și posibil DDoS [S25]	Nu rezultă o concluzie privind sistemele interne
Au fost exportate mesaje sensibile?	Cercetarea descrie capacitatea de colectare	SRI afirmă că nu a identificat exfiltrări sensibile [S7]; ESET descrie comportamentul instrumentelor [S6][S8]	Păstrați fiecare afirmație legată de sursa sa

6.4 Cronologia comunicărilor și afirmațiilor

4 feb 2026 — **Transportator de energie**
Incident IT de afaceri raportat; păstrată excluderea sistemelor operaționale [S20]

13 feb 2026 — **Relatarea sursei**
Modificarea neautorizată a unui site de facultate întrerupe accesul [S79]

14 mar 2026 — **Ministerul de Externe**
Încetinire și întreruperi scurte legate de DDoS la 13–14 martie [S62]

8 apr 2026 — **SRI**
Anunțată participarea la destructurarea rețelei de routere [S9]

3 iul 2026 — **Relatarea sursei**
Defigurarea repetată a unui site public din transporturi [S98]

10 iul 2026 — **Relatarea sursei**
Site-uri ale primăriilor investigate după întreruperea accesului [S88]

16 iul 2026 — **Minister responsabil de finanțare publică**
Aplicație de achiziții indisponibilă după un incident [S22]

27 iul 2026 — **Guvern**
Relatare privind ransomware și recuperarea aplicațiilor administrative publice [S21]

29 iul 2026 — **Administrație penitenciară**
Raportate ransomware, suspendarea serviciilor și izolarea sistemelor [S23]

29 iul 2026 — **Relatarea sursei**
Servicii universitare academice și administrative perturbate [S84][S97]

4 aug 2026	**Relatarea sursei** Intervenție după un atac ransomware la o bancă din România [S77][S78]
18 aug 2026	**Autoritate regională de program** Aplicație de achiziții restabilită; păstrată întreruperea anterioară [S61]
8 sep 2026	**DNSC** Dificultăți temporare ale site-ului; posibil DDoS [S25]
25 sep 2026	**Relatarea sursei** Acces restricționat la un portal guvernamental după sesizări privind datele personale [S85]
16 oct 2026	**Operator al pieței de capital** Comunicat incidentul unei aplicații auxiliare pentru investitori [S26]
19 oct 2026	**Presă națională** Operatorul de comunicații și DNSC descriu un incident în rețeaua internă [S27]
22 oct 2026	**Relatarea sursei** Plăți locale online indisponibile și înlocuirea planificată a sistemului [S89][S90]
29 oct 2026	**Relatarea sursei** Întreruperea serviciilor unei librării și redeschiderea din noiembrie [S82][S83]
30 oct 2026	**Relatarea sursei** O direcție fiscală locală a anunțat atacuri repetate [S87]
3 nov 2026	**Radio național** Raportate posibile incidente frigorifice la șase magazine [S63]
10 nov 2026	**NorthDivision** Acces administrativ la o platformă comercială oferit, neverificat [S1]
10 nov 2026	**ternny** Documente juridice private oferite, neverificate [S1]
10 nov 2026	**Cercetare ESET** Publicată cercetarea instrumentelor de e-mail guvernamental; păstrate datele vechi [S6][S8]
11 nov 2026	**SRI** Descrise detectarea și răspunsul din decembrie 2025 [S7]
17 nov 2026	**ANSPDCP** Publicată constatarea privind ransomware în turism [S33]
18 nov 2026	**Avertizare DNSC relatată** Avertizare privind impersonarea operatorilor mobili și instituțiilor [S28]
20 nov 2026	**Relatarea sursei** Documente accesate printr-un portal de deschidere a conturilor [S80][S96]
21 nov 2026	**Poliție** Publicat studiul fraudei de investiții pentru ianuarie–septembrie [S29]

6.5 Activitate recentă: 8–22 noiembrie

Setul de forum etichetat cu țara conține 14 postări în această perioadă. Cele mai relevante oferte de acces și documente sunt anunțul comercial din 10 noiembrie și oferta de documente juridice. Rămân neverificate. Limitele complete apar în cazurile L și M. [S1]

Dosarul juridic include și o postare din 5 noiembrie, sub același pseudonim. Ea este în afara intervalului recent, dar relevantă pentru cronologia dosarului. Publicările din noiembrie nu stabilesc momentul obținerii documentelor.

Deciziile ANSPDCP din 11, 13 și 17 noiembrie descriu un furnizor de credit, o firmă de servicii energetice și un operator turistic. Sunt publicări recente ale unor constatări. Nu precizează datele atacurilor și nu trebuie transformate în trei intruziuni noi din noiembrie. [S33][S34][S35]

Avertizarea din 18 noiembrie descrie o succesiune de apeluri cu identitatea unui operator mobil, urmată de un pretext instituțional. Răspunsul practic este oprirea procesului impus de apelant și verificarea printr-un canal oficial obținut independent. [S28]

Studiul poliției publicat la 21 noiembrie acoperă plângeri privind fraude de investiții din ianuarie până în septembrie. Actualizează o populație istorică de raportare. Este util controalelor antifraudă, dar distinct de anunțurile curente de forum. [S29]

La 18 noiembrie, un reprezentant BNR a descris un exercițiu de stres cibernetic, incluzând sistemele bancare principale, comunicațiile și efectele adverse ale rețelelor sociale. Este un scenariu de exercițiu, nu dovada că băncile românești au suferit acel eveniment combinat. [S59]

Două cataloage pentru mai multe țări, datate 16 noiembrie, oferă și acces shell și includ site-uri românești. Nu stabilesc proprietatea, accesul curent sau o intruziune nouă în România. Folosiți fiecare referință pentru verificarea proprietății și sesiunilor, fără a o accepta drept acces confirmat. [S1]

Actualizarea unei firme de servicii de investiții din 20 noiembrie a confirmat accesul la baza de date și documente prin portalul de deschidere a conturilor, după un incident datat 30 octombrie. Firma a precizat că activele clienților rămâneau protejate, iar notificarea și evaluarea impactului continuau. Publicarea nu mută incidentul inițial în noiembrie. [S80]

Un e-mail al unei librării a anunțat redeschiderea pe 18 noiembrie după perturbarea din octombrie. Susține recuperarea unui canal de vânzare. Nu stabilește refacerea tuturor serviciilor sau concluziile finale privind datele. [S83]

O comunicare municipală din 16 noiembrie a planificat înlocuirea serviciului de plată online pentru 23 noiembrie. A doua dată este după termenul raportului și nu reprezintă o recuperare observată. Comunicarea recunoaște și probleme de acces la o platformă națională de plată. Un canal alternativ disponibil în octombrie nu poate fi presupus disponibil permanent. [S90]

Poliția a negat explicit un atac cibernetic asupra radarelor la 17 noiembrie și a descris evaluări tehnice. Dezmințirea ajută la respingerea unei afirmații circulate, nu adaugă un atac la totalul cazurilor. Verificați comunicarea sursei înainte de escaladarea unui titlu despre indisponibilitate. [S95]

6.6 Comunicarea faptului stabilit

O primă actualizare utilă precizează serviciul afectat, întreruperea cunoscută, limitele investigației și ora următoarei actualizări. Spuneți dacă sunt stabilite o acuzație, o întrerupere observată, acces neautorizat sau divulgarea datelor. Păstrați precizia formulării responsabilului serviciului.

Canalul alternativ de stare trebuie să funcționeze când e-mailul sau site-ul principal sunt indisponibile. Exersați instrucțiunile pentru clienți fără a cere serviciul defect pentru verificarea identității. Păstrați rutele de contact cunoscute pentru contestarea unei cereri suspecte de modificare.

Pentru sisteme operaționale, includeți responsabilul procesului fizic. Întreruperea unei aplicații publice și o temperatură frigorifică anormală cer dovezi și teste de recuperare diferite. Niciuna nu stabilește autorul doar pentru că altă țară a raportat ceva similar. [S63]

CONCLUZII PRINCIPALE

01

Verificați impactul serviciului separat de anunțul unei grupări sau oferta de acces.

02

Publicările recente pot descrie atacuri vechi, investigații încheiate sau exerciții.

03

Exersați comunicarea independentă și recuperarea specifică serviciului înaintea următoarei afirmații.

CAPITOLUL 07

Grupări, persoane și relații susținute de dovezi

07

ÎNTREBAREA ACESTUI CAPITOL

Ce afirmații despre autori sunt susținute și ce relații trebuie să rămână netrasate?

12

etichete de grupări ransomware în populația înregistrărilor românești

7.1 Harta relațiilor 92
7.2 Turla și Cereal: păstrarea celor două relatări 94
7.3 Matricea comportamentelor din cercetarea publicată 95
7.4 APT28 și operațiunea privind routerele 96
7.5 Ransomware: etichete și vizibilitate regională 98
7.6 Pseudonime și afirmații despre un operator comun 100
7.7 Grupări care revendică DDoS și limitele mărcilor 101
7.8 Transformarea cunoașterii grupării într-o decizie locală 102

CAPITOLUL 07

Grupări, persoane și relații susținute de dovezi

PE SCURT

Dovezile susțin relatări despre spionaj atribuite surselor, etichete ransomware și anunțuri infracționale. Sunt populații separate. ESET și SRI descriu activitate legată de Turla în limite probatorii diferite. SRI raportează și o operațiune privind routere, atribuită APT28. Etichetele și pseudonimele nu leagă acele campanii de anunțurile românești sau întreruperile oficiale. Alegeți controalele din comportamente documentate și dovezi validate local.

7.1 Harta relațiilor

Postare proprie Redistribuire Declarație oficială Relatare publică Observația noastră

ESET

Relatare publică
Atribuire [S6] ↓

Turla

Declarație oficială
Relatare din 11 noiembrie [S7] ↑

SRI

Declarație oficială
Relatare din 8 aprilie [S9] ↓

APT28

Relatare publică
CERT-EU prezintă atribuirea Zscaler [S113] ↓

Operation Neusploit

HOOKEDGE

Relatare publică
Suprapunerea etichetei BlueDelta în cercetarea Insikt Group [S114] ↑

APT28

Ransompedia

own data
7 înregistrări [S3] ↓

Qilin

NorthDivision

Postare proprie
B13 [S1] ↓

B13: ofertă de acces

ternny

Postare proprie
B12 [S1] ↓

B12: documente oferite

313 Team

Postare proprie
B14 [S1] ↓

Afirmații de disponibilitate

Postare proprie
Afirmații cu marcă B15/B19 [S1] ↑

DDoSia / NoName branding

NU EXISTĂ O LEGĂTURĂ DOCUMENTATĂ CU CEILALȚI ACTORI

Fiecare legătură precizează tipul dovezii. Relațiile Ransompedia sunt observații din date proprii privind înregistrările. Cercetarea furnizorului, atribuirea oficială și anunțurile păstrate au roluri diferite. Harta nu stabilește un ecosistem infracțional general sau un operator comun.

Niciun element comun concret nu leagă dosarele comerciale de cazul de e-mail guvernamental. Raportul nu stabilește un operator comun pentru Turla, APT28, Qilin și vânzătorii de pe forumuri. Păstrarea acestor noduri fără legături este parte a evaluării.

7.2 Turla și Cereal: păstrarea celor două relatări

Turla

Relatare despre spionaj | Atribuire ESET și SRI; fără atribuire independentă nouă

ÎN ROMÂNIA, 2026

2026-11-10
Publicarea cercetării ESET

2026-11-11
Publicarea răspunsului SRI

ȚINTE DECLARATE

Caz de e-mail guvernamental cu activitate anterioară

ÎN RELATĂRILE PUBLICE

[S6] Vendor research

[S7] Official response

EVALUAREA NOASTRĂ

Examinați integritatea e-mailului și conturile, păstrând limitele ambelor surse.

ÎNCREDERE
Încrederea privește afirmația precizată

Cercetarea ESET din 10 noiembrie atribuie Cereal grupării Turla cu încredere ridicată. Descrie un caz Exchange guvernamental românesc din decembrie 2025, cu activitate mai intensă la 20 ianuarie 2026. ESET nu a stabilit accesul inițial. [S6][S8]

Declarația SRI din 11 noiembrie afirmă că Centrul Național Cyberint a identificat atacul în decembrie 2025, l-a oprit, a remediat serviciul și nu a identificat exfiltrări de date sensibile. Menționează vulnerabilități sistemice ale sistemelor de operare Microsoft, fără un CVE. [S7]

Afirmațiile trebuie să rămână vizibile împreună. Capacitatea de colectare nu stabilește un volum exportat. Constatarea oficială privind neidentificarea exfiltrării descrie rezultatul investigației, nu dovada universală a absenței. Raportul nu poate rezolva diferențele dintre perioadele de observație sau sferele surselor.

Consecința defensivă este examinarea integrității serverului de e-mail împreună cu accesul privilegiat. Listele de blocare a rețelei nu răspund singure comportamentelor descrise. Stabiliți ce telemetrie ar distinge mentenanța legitimă, încărcarea neobișnuită de cod și accesul neautorizat la mesaje.

7.3 Matricea comportamentelor din cercetarea publicată

Tabelul selectează comportamente numite explicit în documentul ESET. Nu afirmă că fiecare tehnică s-a produs în România sau că o detecție locală a fost testată. [S8]

TEHNICI DESCRISE ÎN CERCETAREA PUBLICATĂ, PE TACTICI

Execuție	Ascundere	Colectare
T1047 Windows Management Instrumentation	T1055.001 Injecție DLL	T1114.002 Colectarea e-mailului la distanță
	T1620 Încărcare reflectivă de cod	T1119 Colectare automată

Comportamente selectate numite de ESET; nu detector testat sau inventar exclusiv românesc. [S8] [S6]

Comportament	ID ATT&CK	Sfera cercetării	Întrebarea apărătorului
Windows Management Instrumentation	T1047	Interogări descrise în cercetare	Activitatea administrativă corespunde unei sarcini aprobate?
Injecție DLL	T1055.001	Injecție într-un proces descrisă de ESET	Telemetria explică activitatea neobișnuită a modulelor?
Încărcare reflectivă de cod	T1620	Încărcarea în memorie a componentelor	Încărcările neobișnuite sunt corelate cu identitatea și serviciul?
Colectarea e-mailului la distanță	T1114.002	Obținerea mesajelor descrisă în cercetare	Accesul poate fi urmărit până la o identitate autorizată?
Colectare automată	T1119	Selectarea și pregătirea mesajelor	Sunt examinate exporturile și acțiunile neobișnuite ale serviciului?

Matricea reprezintă comportamente descrise, nu o regulă de producție. Responsabilul controlului trebuie să testeze orice analiză rezultată față de mentenanța autorizată și componentele legitime de procesare înainte de utilizarea operațională.

7.4 APT28 și operațiunea privind routerele

APT28

Campanii cu routere și Office atribuite de surse | SRI atribuie operațiunea APT28 și GRU

ÎN ROMÂNIA, 2026

2026-03-02
Publicată sinteza oficială Neusploit

2026-04-08
Participarea SRI anunțată

ȚINTE DECLARATE

Campanii distincte cu routere și documente descrise de sursele citate

ÎN RELATĂRILE PUBLICE

[S9] SRI account

[S10] Joint advisory

[S113] Sinteză CERT-EU

[S114] Cercetare Insikt Group

EVALUAREA NOASTRĂ

Verificați configurația routerului și accesul; nu este stabilită o legătură cu Turla.

ÎNCREDERE
Încrederea privește afirmația precizată

SRI a anunțat participarea la operațiunea Masquerade la 8 aprilie. A descris destructurarea unei rețele de atac bazate pe routere, a atribuit activitatea APT28 și GRU și a precizat că aceasta includea entități din România. [S9]

Avertizarea coordonată de FBI descrie setări DNS modificate și riscuri de interceptare a autentificărilor. Numește CVE-2023-50224 în campania mai largă. Nu stabilește folosirea vulnerabilității împotriva fiecărei entități românești și nu o leagă de Cereal. [S10]

NVD descrie divulgarea neautentificată de informații în instalații de routere TP-Link. Înregistrarea și avertizarea producătorului cer tratarea specifică versiunii hardware. Producătorul indică TL-WR841N V8–V12 drept parțial remediat, inclusiv EU_V11_211209 și EU_V12_230317. Acestea nu sunt corecții universale pentru fiecare revizie. [S11] [S12]

Folosiți tabelul curent al producătorului pentru model și regiune. Înlocuiți dispozitivele fără suport când nu există actualizare potrivită, restricționați administrarea și examinați modificările DNS neașteptate. Deținerea unui model din avertizare nu demonstrează un incident românesc.

Cyber Brief pentru februarie al CERT-EU, publicat la 2 martie, prezintă cercetarea Zscaler despre Operation Neusploit. Include România între țările vizate și atribuie activitatea APT28. Sinteza nu indică un număr de victime românești și nu leagă această campanie de Cereal sau de operațiunea cu routere. [S113]

Campania privește CVE-2026-21509. NVD descrie ocolirea locală a unei funcții de securitate Microsoft Office. KB5002713 remediază problema pentru Office 2016 MSI și exclude explicit Click-to-Run. [S111][S112]

Înregistrarea CVE include produsele de mai jos pe sisteme de 32 de biți și x64. Pentru LTSC și Microsoft 365 Apps, trimite la actualizările de securitate aplicabile, nu la un singur build remediat universal. [S116]

Produs și versiuni afectate	Versiunea remediată corespunzătoare
Office 2016 MSI: anterior versiunii 16.0.5539.1001	16.0.5539.1001; KB5002713; nu pentru Click-to-Run [S112][S116] [S118]
Office 2019 Click-to-Run, licențiere în volum: anterior versiunii 16.0.10417.20095	1808, build 16.0.10417.20095 [S116][S118][S119]
Office LTSC 2021: de la 16.0.1 până la actualizarea de securitate aplicabilă	Licențiere în volum: 2108, build 14334.20522 [S116][S117]
Office LTSC 2024: de la 16.0.0 până la actualizarea de securitate aplicabilă	Licențiere în volum: 2408, build 17932.20670 [S116][S117]
Microsoft 365 Apps for Enterprise: de la 16.0.1 până la actualizarea de securitate aplicabilă	Selectați canalul și versiunea de mai jos [S116][S117]

Buildurile LTSC de mai sus și cele Microsoft 365 Apps de mai jos sunt versiunile din 10 februarie 2026 care includ remedierea. Nu sunt prezentate drept primele builduri remediate. [S117]

Canal Microsoft 365 Apps	Versiune remediată: versiune / build
Current Channel	2601 / 19628.20204
Monthly Enterprise Channel	2512 / 19530.20226; 2511 / 19426.20294; 2510 / 19328.20306
Semi-Annual Enterprise Channel	2508 / 19127.20532; 2502 / 18526.20714; 2408 / 17928.20776

Microsoft descrie și protecția printr-o modificare la nivelul serviciului pentru Microsoft 365 Apps și Office 2021 sau ulterior, cu repornirea aplicațiilor. Office 2016 și 2019 necesită actualizarea de securitate. [S118]

Selectați actualizarea curentă pentru ediția, tipul licenței și canalul folosite. Tratați versiunile enumerate drept repere istorice pentru remediere. Nu înlocuiți Click-to-Run cu un pachet MSI sau ediția retail cu un build pentru licențiere în volum. Apoi verificați controalele documentelor și accesul neobișnuit la e-mail.

Cercetarea Insikt Group despre HOOKEDGE descrie campanii de la sfârșitul lui septembrie 2025 până la începutul lui aprilie 2026, inclusiv ținte românești. Furnizorul evaluează asocierea cu BlueDelta cu încredere moderată și descrie suprapunerea cu eticheta APT28. Raportează documente Word cu macrocomenzi și o componentă de acces ascuns pentru Windows. Nu stabilește un total de victime românești și nu leagă activitatea de celelalte campanii prezentate. [S114]

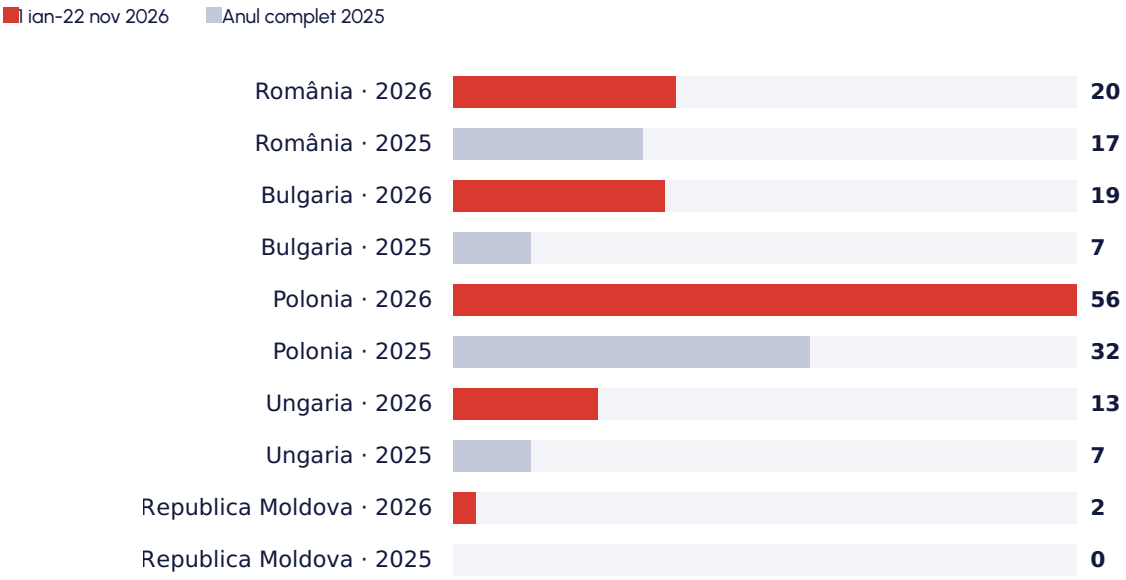
Blocați macrocomenzile din documente cu proveniență nesigură conform politicii aprobate. Verificați sarcinile programate neobișnuite și utilizarea serviciilor web legitime prin dovezi locale. O etichetă comună nu demonstrează infrastructură sau operatori comuni pentru două incidente din România.

7.5 Ransomware: etichete și vizibilitate regională

Ransompedia înregistrează 20 de mențiuni pentru România sub douăsprezece etichete de grupări. Qilin contribuie cu 7, Lockbit5 și Thegentlemen cu câte 2, iar alte nouă etichete cu câte 1. Sunt etichete consemnate, nu atribuirea independentă a fiecărui incident oficial. [S3]

Cele 20 de listări privesc 19 organizații. Rămân evidențe ale afirmațiilor, nu intruziuni confirmate. [S3]

Totalurile regionale ale înregistrărilor descriu vizibilitatea, nu un clasament al riscului



Sursa: afirmații din înregistrările Ransompedia asociate țărilor [S3]. 2026: 1 ianuarie–22 noiembrie, ultima zi parțială; 2025: anul complet. Perioade și vizibilitate diferite; nu reprezintă un clasament național de securitate sau o rată pentru perioade egale.

Țările de comparație au fost selectate ca exemple doar pentru a oferi context; alegerea lor nu implică un clasament sau o evaluare politică.

Țară	Înregistrări în interval	Întregul an 2025	Limita comparației
România	20	17	Anul parțial și anul complet diferă
Bulgaria	19	7	Economie și vizibilitate diferite
Polonia	56	32	Economie regională mai mare; fără ajustare după mărime
Ungaria	13	7	Comparator regional selectat
Moldova	2	0	Populație mai mică; zero descrie această sursă

Comparatorii reflectă vecinătatea, dependențele regionale și contextul limbii române. Cifrele nu măsoară calitatea raportării naționale, pierderile, maturitatea securității sau probabilitatea atacului. O înregistrare poate privi o organizație repetată ori o structură de grup.

O retransmitere din aprilie despre sectorul farmaceutic și retransmiteri din iulie–august despre educație corespund unor listări. Aceasta coroborează publicarea afirmațiilor, nu recunoașterea de către victime. Cele două date din educație privesc o organizație și nu stabilesc două intruziuni. [S1][S3]

O retransmitere din martie despre evidențe ale unei structuri de aplicare a legii nu are o listare nouă corespondentă în 2026 în evidența românească păstrată. O listare anterioară relevantă este datată 2024. Nu confirmă actualitatea, originea sau volumul noii afirmații. Păstrați afirmația separat de un incident verificat. [S1][S3]

Qilin

Etichetă a înregistrărilor ransomware | Fără atribuire independentă către un stat

ÎN ROMÂNIA, 2026

Intervalul 2026

7 înregistrări românești [S3]

ȚINTE DECLARATE

Mai multe etichete sectoriale; organizațiile listate nu sunt numite

ÎN RELATĂRILE PUBLICE

EVALUAREA NOASTRĂ

Șapte înregistrări proprii nu stabilesc șapte intruziuni unice. [S3]

ÎNCREDERE

Încrederea privește afirmația precizată

7.6 Pseudonime și afirmații despre un operator comun

NorthDivision

Pseudonim de vânzător | Coordonarea de către un stat nu este stabilită

ÎN ROMÂNIA, 2026

2026-11-10
Oferta comercială B13

ȚINTE DECLARATE

Platformă comercială generică

ÎN RELATĂRILE PUBLICE

EVALUAREA NOASTRĂ

Anunțul administrativ este păstrat; accesul și vânzarea rămân neverificate. [S1]

ÎNCREDERE
Încrederea privește afirmația precizată

ternny

Pseudonim de vânzător | Coordonarea de către un stat nu este stabilită

ÎN ROMÂNIA, 2026

2026-11-05
Afirmație despre documente

2026-11-10
Oferta de documente B12

ȚINTE DECLARATE

Material juridic privat generic

ÎN RELATĂRILE PUBLICE

EVALUAREA NOASTRĂ

Postările nu validează fișierele, contrapărțile, data obținerii sau vânzarea. [S1]

ÎNCREDERE
Încrederea privește afirmația precizată

Pseudonimele identifică numele folosite în postările păstrate. Un nume persistent poate susține continuitatea publicității, dar autorul, controlul contului și operatorul comun rămân întrebări separate. Formularea similară nu leagă suficient ofertele de acces guvernamental din ianuarie și iunie. [S1]

Dosarul juridic susține două postări observate sub un pseudonim. Nu stabilește același fișier, o vânzare sau acces la fiecare contraparte numită. Dosarul comercial susține existența unui anunț de acces, fără autentificarea independentă a contului.

7.7 Grupări care revendică DDoS și limitele mărcilor

313 Team

Autor de afirmații DDoS | Fără atribuire independentă către un stat

ÎN ROMÂNIA, 2026

2026-03-11
Afirmație despre servicii publice B14

ȚINTE DECLARATE

Site-uri generice de servicii publice

ÎN RELATĂRILE PUBLICE

EVALUAREA NOASTRĂ

Formularea de două ore privește viitorul; durata și impactul nu sunt stabilite independent. [S1]

ÎNCREDERE
Încrederea privește afirmația precizată

DDoSia Project / NoName-labelled accounts

Mărci de campanie în postările păstrate | Coordonarea de stat și operatorul comun nu sunt stabilite independent

ÎN ROMÂNIA, 2026

2026-03
Afirmații de vizare a României B15

2026-08-01
Afirmație despre servicii publice B19

ȚINTE DECLARATE

Servicii publice, transport, energie și finanțe în afirmații

ÎN RELATĂRILE PUBLICE

EVALUAREA NOASTRĂ

Semnăturile și mărcile stabilesc textul observat, nu operatorul sau rezultatul operațional. [S1]

ÎNCREDERE
Încrederea privește afirmația precizată

Postările stabilesc afirmații sub mărcile indicate. Nu stabilesc independent coordonarea de către un stat, identitatea comună a operatorului, acces intern sau relația cu întreruperile oficiale. Relatarea preluată rămâne distinctă de afirmația inițială. [S1]

7.8 Transformarea cunoașterii grupării într-o decizie locală

Folosiți descrierea campaniei pentru alegerea dovezilor examinate. Colectarea mesajelor cere dovezi despre căsuțe și integritatea serverului. Manipularea routerelor cere verificarea proprietății și configurației. O înregistrare de șantaj cere evaluarea continuității și comunicării. Un anunț cere validarea contului și datelor.

Nu folosiți un nume familiar pentru a umple o legătură lipsă. O etichetă ransomware cunoscută nu stabilește criptarea într-un incident public concret. Atribuirea unui stat într-o campanie oficială nu se transferă unei întreruperi sau unui vânzător separat.

CONCLUZII PRINCIPALE

01
Atribuiți fiecare evaluare despre state și autori sursei sale.

02
Etichetele ransomware, pseudonimele și campaniile oficiale rămân separate.

03
Construiți controale pe comportamente documentate și verificare locală, fără a presupune un operator comun.

CAPITOLUL 08

Economia fraudei

08

ÎNTREBAREA ACESTUI CAPITOL

Cum pot deveni datele personale o instrucțiune sau tranzacție neautorizată?

3

întrebări distincte: identitate, autoritate și tranzacție

8.1 Informația nu înseamnă autoritate 104

8.2 Materialul privind cardurile: sferă restrânsă 104

8.3 Conturi, verificare și reutilizarea documentelor 105

8.4 Prețurile cerute nu reprezintă valoarea pieței 105

8.5 Observații oficiale despre campanii 105

8.6 Avertizări pentru investitori și aplicarea transfrontalieră a legii 107

8.7 Transfer practic către echipele antifraudă 107

CAPITOLUL 08

Economia fraudei

PE SCURT

Anunțurile asociate României combină date de identitate, conturi și afirmații de acces. Avertizările oficiale descriu impersonare, fraude de investiții și abuzul conturilor sociale. Un nume, o factură sau un document autentic poate face cererea credibilă fără a o autoriza. Populația restrânsă de carduri nu măsoară frauda națională. Testați recuperarea conturilor, schimbarea beneficiarilor și contactul cu clienții față de un adversar care cunoaște deja date personale.

8.1 Informația nu înseamnă autoritate

Ofertele păstrate descriu informații despre clienți, companii, facturi, educație și documente juridice. Dacă sunt autentice, acestea pot susține o abordare convingătoare. Nu autorizează schimbarea destinației plății, recuperarea contului sau divulgarea altor documente. [S1]

Construiți verificarea în jurul acțiunii solicitate. Numele clientului poate ajuta la găsirea unei înregistrări, dar o schimbare sensibilă cere dovadă independentă de autoritate. Folosiți un contact stabilit înaintea cererii suspecte și evitați noul număr sau adresa oferite în ea.

Distincția contează pentru asistență și trezorerie. O persoană care încearcă recuperarea frauduloasă poate cunoaște comanda sau descrierea documentului. Personalul trebuie să știe ce fapte ajută la căutare și ce controale autorizează o modificare.

8.2 Materialul privind cardurile: sferă restrânsă

SFERA CIFRELOR DIN FIȘE

Cifrele acoperă numai carduri de plată apărute în clar în postările clandestine colectate pentru raport. Brandefense detectează carduri furate prin multe alte metode, în afara acestui raport. Cifrele nu măsoară furtul, valabilitatea cardurilor sau pierderile din fraudă.

Populația postărilor păstrate conține 94 de carduri distincte asociate României în 107 de postări. Observațiile nu stabilesc valabilitatea curentă sau efectuarea unei plăți. [S4]

Eșantionul nu permite estimarea întregii expuneri a cardurilor din România sau recomandarea reemiterii generale. Emitentul trebuie să verifice starea contului, tranzacțiile încercate și dovezile proprii de fraudă înainte de măsuri pentru clienți. Statutul de aprobare pretins de autor nu confirmă o plată reușită.

8.3 Conturi, verificare și reutilizarea documentelor

Dosarul conturilor de consumatori include cereri de ocolire a verificării identității și instrumente pentru verificarea conturilor. Cererea stabilește interesul, fără a demonstra o capacitate funcțională. Oferta de fotografii nu identifică sistemul sursă și nu dovedește o pierdere nouă dintr-un registru al statului. [S1]

Pentru un serviciu care folosește documente, testați recuperarea și înscrierea față de imagini reutilizate și date personale cunoscute. Examinați excepțiile, încercările repetate și schimbările datelor de contact. Dovada finalizării trebuie să demonstreze decizia de autorizare, nu doar încărcarea unui document.

Nu interpretați limba postării drept naționalitatea autorului. Engleza și rusa pot fi limbi ale pieței. Referințele la țară pot descrie clienți deserviți sau piețe de plăți, nu locul intruziunii.

Alte postări oferă sau caută conturi asociate unor bănci, predarea conturilor și capacitate de primire a plăților. Fluxurile recurente pretinse nu stabilesc transferuri, acces valid, intruziuni bancare sau pierderi. Echipele antifraudă trebuie să verifice titularul și autoritatea plății separat de identitatea autorului anunțului. [S1]

8.4 Prețurile cerute nu reprezintă valoarea pieței

Observație	Unitatea oferită	Preț	Limită
Oferta din ianuarie despre un comerciant de modă	Set pretins de 84.792 de linii	200 USD	Data postării și data intruziunii pretinse se contrazic; autenticitate și vânzare neverificate
Oferta de date din mai	Bază pretinsă de 86.283 de linii	300 USD	Preț cerut; autenticitatea și vânzarea neverificate
Căutări despre vehicule în noiembrie	1.000 de căutări	10 USD	Serviciu promovat; autoritatea sursei neverificată

Sursă: anunțurile păstrate [S1]. Ofertele au unități diferite și nu susțin un preț median comun. Nici prețul vizibil, nici răspunsul nu demonstrează o plată.

Un preț mic nu dovedește fabricarea. Un preț mare nu dovedește calitatea sau accesul curent. Tratați numărul, prețul și actualitatea ca afirmații separate, care cer dovezi.

8.5 Observații oficiale despre campanii

Tabelul urmează data publicării. Rândurile descriu avertizări ori investigații, nu atacuri noi confirmate la acele date.

Publicat	Relatarea sursei	Limita dovezilor	Decizie defensivă
26 ianuarie	Avertizare DNSC relatată despre SMS și mesagerie cu pretext de curierat [S54]	Avertizare, nu inventar de victime	Verificați livrarea în serviciul cunoscut
11 februarie	Avertizare DNSC relatată despre taxe de marcă [S56]	Pretext de plată, nu intruziune la registrator	Verificați independent autoritatea și factura
17 aprilie	Avertizare relatată despre identități instituționale în phishing [S55]	Numele autorității nu o face autorul atacului	Verificați solicitările printr-un canal cunoscut
8 iulie	Investigație a poliției privind conturi comerciale [S30]	Fapte presupuse aflate în investigație	Examinați recuperarea contului și mesajele tranzacției
5 august	SRI avertizează despre falsificarea identității apelantului [S31]	Numărul afișat nu autentifică apelantul	Reapelați folosind date verificate independent
9 august	Avertizare a poliției privind vishing [S32]	Avertizare, nu total de transferuri reușite	Respingeți accesul la distanță și instrucțiunile dictate
18 noiembrie	DNSC avertizează despre impersonare succesivă a operatorului mobil și unei instituții [S28]	Autoritatea pretinsă face parte din pretext	Opriți secvența și verificați separat
18 noiembrie	Relatare privind investigația DIICOT asupra phishingului social [S53]	Activitate presupusă din septembrie 2024–ianuarie 2025	Verificați recuperarea și avertizați contactele după abuz confirmat
21 noiembrie	Studiul poliției privind fraude de investiții în ianuarie–septembrie [S29]	Plângeri retrospective, nu incidența din noiembrie	Pregătiți escaladarea și păstrarea dovezilor

Poliția a raportat 1.624 de plângeri în studiul pentru ianuarie–septembrie. A descris peste 73,6 milioane RON în 1.346 de situații și aproximativ 8,5 milioane EUR în 260 de situații. Categoriile valutare și situațiile nu trebuie adunate ca victime unice. [S29]

Studiul susține un răspuns de afaceri: clienții au nevoie de o cale pentru a contesta oportunitățile de investiții sau instrucțiunile de transfer înainte de plată. După un transfer suspect, păstrați comunicările și istoricul tranzacției și folosiți canalul antifraudă stabilit al instituției.

Avertismentele suplimentare păstrează aceeași distincție între capcana pentru clienți și intruziunea într-o instituție.

Publicat	Relatarea sursei	Limita dovezilor	Decizia defensivă
2 aprilie	Apeluri de impersonare a autorității fiscale folosesc nume publice pentru a cere date personale sau bancare; avertisment regional la 20 mai [S91][S92]	Pretext de identitate; intruziune în sistemele autorității nestabilită	Verificați cererea printr-un canal oficial obținut independent
7 mai	Autoritatea pentru digitalizare avertizează despre SMS-uri către pagini clonate de plăți pentru cetățeni [S101]	Avertisment, nu dovada intruziunii în platforma legitimă	Deschideți independent serviciul cunoscut și verificați autoritatea plății
23 mai	Furnizor de energie avertizează despre phishing cu plata facturilor [S102]	Avertisment pentru clienți; intruziune în rețeaua furnizorului nestabilită	Verificați originea facturii și modificările plății prin contacte cunoscute
4 august	Autoritatea poștală descrie pretexte despre taxe de livrare, adrese, dulapuri de colетărie și conturi de mesagerie [S93]	Avertismentul sectorial nu stabilește o intruziune la curier	Refuzați asocierea conturilor la cererea apelantului și verificați prin serviciul cunoscut
24 august	O redacție primește e-mailuri de impersonare a unei bănci [S103]	Mesaj observat de presă; amploarea și intruziunea bancară nedovedite	Verificați independent cererile despre dispozitive și autentificare
5 octombrie	O publicație tehnologică descrie o capcană de rambursare trimisă de un cititor [S104]	Furtul reușit și intruziunea la comerciant nu sunt stabilite	Verificați rambursările în serviciul cunoscut al comerciantului sau plăților

8.6 Avertizări pentru investitori și aplicarea transfrontalieră a legii

Registrul ASF conține avertizări datate despre servicii de investiții neautorizate sau înșelătoare. Avertizarea este un semnal pentru verificare, nu atribuirea fiecărui mesaj fraudulos cu o marcă similară. Confirmați entitatea juridică și serviciul autorizat din informațiile actuale ale autorității. [S57]

O actualizare a poliției din noiembrie descrie presupuse fraude pe o platformă fiscală, cu percheziții în România și un serviciu afectat din străinătate. Este aplicare transfrontalieră a legii, nu dovada expunerii clienților români. Suspiciunile rămân supuse investigației. [S52]

8.7 Transfer practic către echipele antifraudă

Stabiliți ce trimite securitatea către prevenirea fraudei: relația validată cu un cont sau o înregistrare, acțiunea posibilă, date relevante și incertitudini. Evitați folosirea unui volum mare, necalificat, ca instrucțiune pentru blocarea clienților.

Echipele pentru clienți răspund de avertizări și reapelare sigură. Trezoreria răspunde de schimbarea beneficiarului. Identitatea răspunde de conturi și sesiuni. Protecția datelor evaluează evidențele afectate. Coordonatorul incidentului reconciliază deciziile fără să transforme fiecare semnal în același răspuns.

CONCLUZII PRINCIPALE

01

Informația autentică nu stabilește autoritatea pentru o modificare sensibilă.

02

Observațiile cardurilor și prețurile au unități restrânse și nu măsoară pierderile naționale.

03

Reuniți identitatea, prevenirea fraudei și relațiile cu clienții în jurul dovezilor validate și contactelor sigure.

CAPITOLUL 09

Sectorul bancar și serviciile financiare

09

ÎNTREBAREA ACESTUI CAPITOL

Ce controale financiare rezultă din dovezi fără exagerarea expunerii?

30

domenii financiare candidate selectate, nu treizeci de bănci independente verificate

9.1 Populație și limite 110

9.2 Autoritatea angajatului cere dovada scopului profesional 110

9.3 Erorile de prelucrare și atacurile cer remedieri diferite 111

9.4 Contextul plății nu înseamnă autoritate de plată 111

9.5 Servicii pentru clienți și funcții critice ale pieței 111

9.6 Scenariul de stres cibernetic rămâne un scenariu 112

9.7 Responsabilitate comună și raportare 112

CAPITOLUL 09

Sectorul bancar și serviciile financiare

PE SCURT

Serviciile financiare cer controale separate pentru angajați, clienți, furnizori și autoritatea tranzacțiilor. Cele 30 de domenii financiare candidate conțin cel puțin 10.503 de asocieri de dispozitive și 63.106 de evidențe de autentificare. Deciziile oficiale descriu acces neautorizat al angajaților, erori de notificare și un atac IT. Discuția din noiembrie despre stres cibernetic privește un exercițiu, nu un incident bancar. Verificați accesul, protejați schimbarea plăților și testați serviciile pentru clienți alături de recuperarea tehnică.

9.1 Populație și limite

Grupa financiară cuprinde 30 de domenii candidate. Include autorități, infrastructuri de piață, servicii de plăți și investiții, alături de bănci. Nu este un inventar de emitenți autorizați sau treizeci de bănci independente. Proprietatea domeniului și independența entității rămân limite ale selecției. [S2]

Portofoliul financiar conține cel puțin 10.503 de asocieri de dispozitive, inclusiv 284 de asocieri ale dispozitivelor angajaților, și 63.106 de evidențe de autentificare. Ofertele curente privesc 9 dintre cele 30 de domenii. Observațiile suprapuse nu stabilesc conturi active ale clienților, pierderi din fraudă sau intruziuni confirmate. [S2]

Observațiile cardurilor includ 26 de carduri sub 7 etichete financiare. Etichetele nu stabilesc statutul de emitent autorizat. Verificarea contului și emitentului trebuie să preceadă măsurile pentru clienți. [S2][S4]

SFERA CIFRELOR DIN FIȘE

Cifrele despre carduri menționate aici acoperă numai cardurile vizibile în clar în postările colectate. Brandefense detectează carduri furate prin multe alte metode, în afara raportului. Cifrele nu măsoară furtul, valabilitatea sau pierderile din fraudă.

Populația separată de carduri conține 94 de carduri în 107 de postări, cu limitele de mai sus. Nu reprezintă expunerea domeniilor financiare selectate. Observațiile cardurilor cu etichete financiare nu stabilesc un incident în infrastructura emitentului. [S4]

9.2 Autoritatea angajatului cere dovada scopului profesional

Constatarea ANSPDCP din 2 iulie descrie accesul unui angajat la extrase de cont în afara atribuțiilor, la cererea unui terț. Și decizia ANSPDCP din noiembrie privește depășirea autorizării angajaților. Sunt constatări de guvernanță a accesului, nu o campanie externă comună. [S40][S41]

Examinați consultările neobișnuite ale înregistrărilor alături de rol, repartizarea cazului și scopul profesional. Accesul privilegiat nu este automat legitim fiindcă angajatul s-a autentificat. Păstrați explicații auditabile pentru excepții și o cale de investigare fără circulația inutilă a datelor clienților.

9.3 Erorile de prelucrare și atacurile cer remedieri diferite

Decizia din 29 mai descrie prelucrarea manuală care a trimis informații de reînnoire a asigurării către destinatari greșiți. Include o constatare separată privind notificarea întârziată. Controalele relevante includ asocierea destinatarilor, verificări de calitate și evaluarea promptă a luării la cunoștință. Răspunsul exclusiv antimalware nu ar rezolva cauza. [S39]

Constatarea din noiembrie privind furnizorul de credit descrie un atac IT și protecția insuficientă a datelor personale. Sfera sa trebuie să orienteze verificarea accesului și recuperarea. Nu stabilește expunerea fiecărei bănci sau rata națională a atacurilor financiare. [S35]

9.4 Contextul plății nu înseamnă autoritate de plată

Ofertele de facturi și date despre clienți pot face instrucțiunile frauduloase plauzibile. O referință, o companie sau un sold corect nu autorizează un beneficiar nou. Folosiți o cale convenită anterior pentru confirmarea modificării, cu al doilea responsabil pentru plăți sensibile. [S1]

Recuperarea clienților cere aceeași disciplină. Modificarea telefonului sau e-mailului pentru aprobare poate transfera autoritatea fără schimbarea parolei. Testați fluxul real și dovezile instituției, fără a presupune că un control de autentificare protejează fiecare decizie.

O relatare de monitorizare din 14 septembrie a susținut că sisteme ale autorităților italiene au fost folosite pentru a solicita date despre clienții unui serviciu financiar. Relatarea a inclus rezidenți români într-o listă mai largă de țări. Niciun subset de date românești nu a fost validat. Este o afirmație despre abuzarea unui canal de divulgare, fără dovezi în acest material privind pătrunderea în sistemele serviciului financiar. [S1]

9.5 Servicii pentru clienți și funcții critice ale pieței

Incidentul aplicației auxiliare pentru investitori ilustrează o distincție utilă. Declarația operatorului păstrează funcționarea și integritatea serviciilor critice de decontare și registru. Aplicația publică și întrebările despre datele clienților rămân separate. [S26]

Exercițiul trebuie să ceară dovezi de la ambii responsabili: operațiunile pieței pentru funcțiile critice și echipele pentru clienți ori protecția datelor pentru conturi. Declarația despre o suprafață nu trebuie să închidă tacit investigarea celeilalte.

Cazul ulterior al portalului unei firme de servicii de investiții arată concret această limită. Protejarea activelor clienților nu stabilește că documentele pentru deschiderea conturilor erau inaccesibile persoanelor neautorizate. Firma a confirmat accesul la baza de date și documente, iar amploarea rămânea neclarificată. Testați separat deschiderea conturilor, tranzacționarea și custodia și păstrați dovezi distincte pentru evaluarea vieții private. [S80]

9.6 Scenariul de stres cibernetic rămâne un scenariu

Discuția BNR relatată la 18 noiembrie descrie un exercițiu care combină pierderea sistemelor IT principale și a unui canal de comunicare cu efecte adverse pe rețelele sociale. Analizează transformarea unui eveniment operațional în problemă de lichiditate. Este context de planificare, nu un atac combinat raportat. [S59]

Pentru o ipoteză similară, testați împreună accesul la plăți, contactul cu clienții, informațiile de lichiditate și autoritatea deciziei. Consemnați serviciul minim disponibil, cine aprobă tranzacții excepționale și cum primesc clienții o actualizare credibilă.

9.7 Responsabilitate comună și raportare

Decizie	Responsabil	Dovada finalizării
Limitarea conturilor și sesiunilor	Identitate și securitate operațională	Sferă validată și decizii asupra sesiunilor
Contact suspect cu un client	Fraudă și relații cu clienții	Escaladare și reapelare sigură testate
Schimbare sensibilă de plată	Trezorerie sau operațiuni de plată	Verificare independentă și aprobare
Accesul personalului la informații	Responsabil date și conformitate	Analiza scopului profesional și excepțiilor
Restabilirea serviciului	Responsabilul serviciului de afaceri	Test cu acceptarea fluxului clientului
Notificarea supraveghetorului	Juridic și responsabil desemnat	Regim aplicabil, momentul cunoașterii și informațiile trimise

Raportarea DORA, obligațiile de securitate cibernetică civilă și cele privind datele personale cer decizii proprii de aplicabilitate. Echipa trebuie să păstreze o singură cronologie factuală și să aplice ruta corectă fiecărei obligații. Capitolul 10 explică distincțiile. [S13][S14][S15][S60]

CONCLUZII PRINCIPALE

01

Separați deciziile privind angajații, clienții, furnizorii și autoritatea tranzacțiilor.

02

Abuzul de acces și erorile de prelucrare cer controale alături de detecția atacurilor externe.

03

Testați comunicarea cu clienții, funcțiile critice și raportarea împreună cu recuperarea.

CAPITOLUL 10

Reglementare și răspuns național

10

ÎNTREBAREA ACESTUI CAPITOL

Ce obligații se aplică și cum evită organizația folosirea unui termen greșit?

6 ore

maximul pentru raportarea informațiilor transfrontaliere prevăzute la articolul 15(3)

10.1 Citirea actului împreună cu modificarea 114
10.2 Termenele de raportare în securitatea cibernetică civilă 114
10.3 Sancțiunile depind de încălcare 115
10.4 Raportarea datelor personale rămâne separată 116
10.5 DORA și raportarea financiară 116
10.6 Exersarea unui incident cu mai multe obligații 116

CAPITOLUL 10

Reglementare și răspuns național

PE SCURT

Cadrul românesc de securitate cibernetică civilă, GDPR și DORA au sfere, declanșatori și destinatari diferiți. Cadrul cibernetic include un termen specific pentru informații transfrontaliere, alături de avertizarea timpurie și notificarea incidentului. Entitățile financiare cer distincția de aplicabilitate DORA. Cazurile de sancționare arată că și erorile de prelucrare pot crea obligații de notificare. Identificați entitatea, regimul, momentul luării la cunoștință și responsabilul înainte de exersarea primei raportări.

10.1 Citirea actului împreună cu modificarea

Ordonanța de urgență 155/2024 stabilește cadrul românesc de securitate cibernetică civilă. Legea 124/2025 a aprobat-o cu modificări. Ordonanța și modificarea promulgată trebuie citite împreună; un rezumat anterior poate omite sancțiuni sau obligații de conducere schimbate. [S13][S14]

Articolul 2 exclude anumite instituții de apărare, ordine publică, securitate națională și aplicare a legii, precum și sisteme clasificate. Tratamentul entităților supuse DORA este distinct. Excluderile nu justifică presupunerea că toate instituțiile publice sau domeniile financiare candidate urmează aceeași rută. [S13]

Echipa juridică trebuie să consemneze clasificarea entității și serviciului, autoritatea competentă și normele de aplicare relevante. Capitolul este un ghid operațional, nu înlocuiește analiza juridică specifică entității.

10.2 Termenele de raportare în securitatea cibernetică civilă

Tabelul rezumă articolul 15. Fiecare termen își păstrează declanșatorul. Raportarea trebuie făcută prompt, perioada indicată fiind limita maximă. [S13]

Declanșator	Etapă cerută	Maxim	Distincție importantă
Cunoașterea informațiilor care permit echipei naționale constatarea impactului trans-frontalier	Raportarea informațiilor transfrontaliere	6 ore	Obligație specifică din articolul 15(3)
Cunoașterea unui incident semnificativ	Avertizare timpurie	24 de ore	Suspiciuni de activitate rău-voitoare sau impact trans-frontalier, după caz
Cunoașterea unui incident semnificativ	Raportarea incidentului	72 de ore	Gravitate, impact și indicatori disponibili
Solicitarea echipei naționale	Actualizare intermediară	Conform solicitării	Separată de raportarea fina-lă

Declanșator	Etapă cerută	Maxim	Distincție importantă
Transmiterea raportării incidentului	Raport final	O lună	Incident, cauză probabilă, măsuri și impact transfrontalier
Incident în desfășurare la etapa finală	Raport de progres, apoi raport final	Final în termen de o lună de la gestionarea incidentului	Nu omiteți calea pentru incidentul continuu
Incident semnificativ care afectează servicii de încredere	Raportarea incidentului de servicii de încredere	24 de ore	Excepție de la etapa obișnuită de 72 de ore

Ordonanța identifică platforma națională de raportare pentru ruta civilă. Organizația trebuie să stabilească accesul și responsabilul de rezervă înaintea incidentului. Afirmația unui forum nu stabilește automat un incident semnificativ; păstrați evaluarea și cronologia luării la cunoștință. [S13]

10.3 Sancțiunile depind de încălcare

Legea 124/2025 schimbă intervalele sancțiunilor din articolul 60. Cele mai mari intervale se aplică unor încălcări precizate, nu fiecărei întârzieri sau fiecărui incident. Cifra de afaceri este cea anuală mondială din ultimul exercițiu financiar. [S14]

Entitate sau categorie	Intervalul prevăzut	Limită
Entități importante, încălcările articolului 60(2)(a)	De la 5.000 RON la echivalentul a 7.000.000 EUR sau 1,4% din cifra mondială anuală, maximul mai mare	Se aplică literelor enumerate
Entități esențiale, încălcările articolului 60(2)(b)	De la 10.000 RON la echivalentul a 10.000.000 EUR sau 2% din cifra mondială anuală, maximul mai mare	Se aplică literelor enumerate
Entități importante, articolul 60(2)(c)	1.000–300.000 RON	Alte încălcări enumerate
Entități esențiale, articolul 60(2)(d)	1.500–500.000 RON	Alte încălcări enumerate
Categoria articolului 60(2)(e)	1.000–100.000 RON	Alte încălcări enumerate
Încălcări grave conform articolului 60(2¹)	3.000–600.000 RON	Majorarea pentru repetare și individualizarea cer condițiile legale

Nu prezentați amenda maximă drept estimare a pierderii din incident. Conducerea și responsabilul raportării trebuie să demonstreze clasificarea, controalele cerute și promptitudinea răspunsului.

10.4 Raportarea datelor personale rămâne separată

Întrebările frecvente oficiale ANSPDCP precizează notificarea de către operator fără întârzieri nejustificate și, dacă este posibil, în 72 de ore de la cunoaștere. Excepția privește încălcarea improbabil să genereze un risc pentru drepturile și libertățile persoanelor. [S15]

Decizia bancară din mai ilustrează constatarea separată a notificării întârziate, alături de deficiențele de securitate. Cauza a fost o eroare de prelucrare, nu un atac extern stabilit. Coordonatorul trebuie să transmită echipei de protecție a datelor și evenimentele de livrare greșită ori control al accesului. [S39]

Consemnați momentul cunoașterii, datele afectate, decizia privind riscul și informațiile disponibile la fiecare etapă. Investigația în curs a furnizorului nu răspunde singură întrebării proprii a operatorului despre raportare.

10.5 DORA și raportarea financiară

Prezentarea oficială ASF precizează aplicarea DORA de la 17 ianuarie 2025. Descrie raportarea incidentelor TIC majore către autoritatea competentă relevantă și informarea fără întârziere a clienților ale căror interese financiare sunt afectate. [S60]

Articolul 2(3) al cadrului civil păstrează doar articolele 5–10 și 18 pentru entitățile financiare supuse DORA. Nu aplicați succesiunea articolului 15 fiecărei bănci fără verificarea sferei. Confirmați ruta relevantă BNR sau ASF pentru entitate. [S13][S14]

Regulamentul delegat 2025/301 distinge cunoașterea de clasificarea ca major. Etapa inițială este cât mai rapidă, în 4 ore de la clasificare și cel târziu în 24 de ore de la cunoaștere. Clasificarea ulterioară are o regulă specifică de 4 ore. [S67]

Raportul intermediar este datorat în 72 de ore de la notificarea inițială. Cel final urmează în termen de o lună de la cel mai recent intermediar. Regulamentul include prevederi pentru weekenduri, sărbători și tipuri de entități; responsabilul trebuie să le verifice, fără a presupune o prelungire universală. [S67]

10.6 Exersarea unui incident cu mai multe obligații

Dați echipei o alertă de acces, un serviciu indisponibil pentru clienți și copiere incertă de date personale. Cereți identificarea entității, clasificarea, consemnarea cunoașterii și alegerea destinatarului. Nu așteptați atribuirea finală pentru evaluarea obligației de raportare.

Cereți responsabilului juridic sau de raportare să explice fiecare termen. Păstrați aceleași fapte în notificările de date, securitate și financiare, cu teste legale diferite. Dovada finalizării este decizia consemnată și ruta utilizabilă, inclusiv responsabilul din afara programului.

CONCLUZII PRINCIPALE

01

Verificați entitatea și regimul înainte de alegerea termenului.

02

Păstrați distincțiile pentru informații transfrontaliere, servicii de încredere și DORA.

03

Oferiți responsabililor de raportare, date și comunicare o cronologie unică și decizii juridice separate.

CAPITOLUL 11

Perspective

11

ÎNTREBAREA ACESTUI CAPITOL

Ce evaluări rezultă din dovezi și ce le-ar modifica?

4

scenarii condiționale cu declanșatori expliciți

11.1 Evaluări principale 119
11.2 Ce ar modifica evaluarea 120
11.3 Scenarii condiționale de planificare 120
11.4 Ce nu pot prognoza datele 120

CAPITOLUL 11

Perspective

PE SCURT

Dovezile susțin pregătirea pentru abuz de identitate, pierderea documentelor la furnizori și perturbarea serviciilor. Nu susțin o probabilitate națională a atacului sau ierarhizarea securității sectoarelor. Publicările recente pot dezvălui activitate veche, iar anunțurile pot recircula date istorice. Folosiți scenarii condiționale cu declanșatori măsurabili și schimbați răspunsul când un cont validat, un set de date confirmat sau impactul serviciului modifică dovezile.

11.1 Evaluări principale

Evaluare	Încredere și bază	Limită	Răspunsul responsabilului
Accesul administrativ merită un proces cu responsabil desemnat	Ridicată pentru anunțurile observate și constatările oficiale de acces [S1][S37]	Oferta nu stabilește acces funcțional	Identitatea investighează privilegiile și sesiunile
Documentele pot susține fraude ulterioare cu origine încă incertă	Moderată, deducție din tipurile de înregistrări oferite [S1]	Nu se deduc pierderi realizate	Responsabilii fraudei și datelor testează autoritatea și contactul
Recuperarea trebuie să includă aplicațiile și fluxurile clienților	Ridicată pentru întreruperi și limitele restabilirii [S21][S22] [S26][S61]	Un caz nu estimează capacitatea națională	Responsabilul acceptă restabilirea demonstrată
Relatarea recentă despre spionaj justifică examinarea integrității e-mailului	Ridicată pentru existența relatărilor [S6][S7][S8]	Perioadele și sferele rezultatului diferă	SOC și echipa de e-mail stabilesc dovezile locale necesare
Avertizările privind procese fizice merită verificare delimitată	Moderată pentru posibilele incidente frigorifice relatate [S63]	Mecanismul și pierderile românești rămân neclarificate	Operațiunile verifică echipamentele, alarmele și furnizorii

Încrederea privește afirmația, nu vânzătorul sau gruparea în ansamblu. Încrederea ridicată că un anunț există poate coexista cu încredere redusă în conținutul său.

11.2 Ce ar modifica evaluarea

Dovadă nouă	Schimbarea evaluării	Decizie
Contul oferit corespunde unor sesiuni active neautorizate	Afirmația devine incident local de identitate	Limitați sesiunile validate și investigați privilegiile conexe
Verificări interne autorizate validează evidențe sensibile	Afirmația capătă o bază locală concretă	Stabiliți sfera și evaluați protecția persoanelor și clienților
Telemetria confirmă întreruperea unui serviciu de afaceri	Afirmația de disponibilitate capătă impact măsurat	Activați continuitatea și escaladarea furnizorului
O declarație oficială schimbă sfera datelor sau recuperării	Relatarea preliminară cere actualizare	Reconciliați comunicarea, notificarea și controalele
Un element tehnic concret leagă campanii	O relație specifică poate fi susținută	Documentați legătura și păstrați atribuirea sursei

Potrivirea unui eșantion justifică investigarea înaintea acceptării întregului volum sau a datei pretinse. O constatare negativă într-o sursă nu demonstrează absența activității în altă parte.

11.3 Scenarii condiționale de planificare

Sunt ipoteze de planificare, nu predicții sau probabilități.

1. **Dacă o ofertă administrativă corespunde unui cont curent**, verificați imediat sesiunile și privilegiile prin responsabilul contului. Escaladați activitatea neautorizată confirmată și evaluați separat accesul la date.
1. **Dacă un furnizor confirmă pierderea documentelor sensibile**, identificați înregistrările și clienții implicați. Contestați instrucțiunile juridice și de plată prin căi cunoscute și evaluați notificarea din sfera confirmată.
1. **Dacă accesul la un serviciu public este perturbat**, activați fluxul alternativ testat și canalul independent de stare. Măsurați recuperarea prin sarcini reușite ale utilizatorilor, fără a interpreta întreruperea ca dovadă de acces la date.
1. **Dacă setările procesului fizic se modifică neașteptat**, implicați operațiunile și responsabilul echipamentului. Păstrați dovezile în siguranță, verificați furnizorii și restabiliți configurația testată. Nu transferați atribuirea dintr-o relatare străină similară.

11.4 Ce nu pot prognoza datele

Volumele postărilor, înregistrările sursei și portofoliul selectat nu produc o probabilitate națională a incidentului. Volumele oferite nu prognozează pierderile din fraudă. Afirmația unei surse privind lipsa impactului nu stabilește rezultatul tuturor organizațiilor cu tehnologie similară.

Perspectiva utilă este un declanșator probatoriu legat de un responsabil. Revizuiți-l după comunicări noi, verificați schimbările în aceeași unitate și păstrați distincția dintre actualizare și alt incident.

CONCLUZII PRINCIPALE

01

Atribuiți fiecărei evaluări o limită a sursei și un semnal de schimbare.

02

Folosiți accesul, datele și impactul validate pentru acțiuni specifice.

03

Reevaluați după comunicări ulterioare fără a transforma actualizările în incidente suplimentare.

CAPITOLUL 12

Plan de acțiune

12

ÎNTREBAREA ACESTUI CAPITOL

Cine acționează în 30, 60 și 90 de zile și ce demonstrează finalizarea?

18

acțiuni cu responsabili și dovezi observabile

12.1 Planul pe 30/60/90 de zile 123
12.2 Responsabilitatea pe roluri 125
12.3 Indicatori de finalizare 125
12.4 Cum poate ajuta Brandefense 126

CAPITOLUL 12

Plan de acțiune

PE SCURT

Începeți prin a confirma că alertele despre conturi și acces ajung la echipa potrivită. Verificați privilegiile, furnizorii și fluxurile sensibile înainte de măsuri perturbatoare. Apoi testați politica de e-mail, administrarea, schimbările plăților și serviciul minim. Până în ziua 90, demonstrați recuperarea și un exercițiu de raportare care reunește deciziile tehnice, juridice și pentru clienți. Închideți fiecare acțiune cu dovezi acceptate de responsabilul de afaceri.

12.1 Planul pe 30/60/90 de zile

1Zilele 1–30

Confirmați livrarea alertelor de cont și acces pentru serviciile proprii

RESPONSABIL
CISO și identitate

DOVADA FINALIZĂRII
Alertă de test primită și repartizată

Verificați ofertele noi față de conturi active

RESPONSABIL
Identitate

DOVADA FINALIZĂRII
Evidența contului, sesiunii și deciziei

Identificați deținătorii documentelor sensibile și permisiunile de export

RESPONSABIL
Responsabili date și achiziții

DOVADA FINALIZĂRII
Hartă aprobată a serviciilor și furnizorilor

Inventariați administrarea, inclusiv furnizorii și urgențele

RESPONSABIL
Infrastructură

DOVADA FINALIZĂRII
Responsabil pentru fiecare cale aprobată

Stabiliți clasificarea entității și rutele de raportare

RESPONSABIL
Juridic și conformitate

DOVADA FINALIZĂRII
Aplicabilitate semnată și raportor de rezervă

Pregătiți canal independent de stare și contact sigur

RESPONSABIL
Comunicare și responsabili servicii

DOVADA FINALIZĂRII
Test fără e-mailul sau site-ul obișnuit

2Zilele 31–60

Protejați administrarea cu MFA potrivit și permisiuni restrânse

RESPONSABIL

Infrastructură și identitate

DOVADA FINALIZĂRII

Test autorizat și responsabilul excepției

Examinați telemetria căsuțelor privilegiate și integrității serverului

RESPONSABIL

SOC și responsabil e-mail

DOVADA FINALIZĂRII

Surse de dovezi și procedură testată

Introduceți politica de e-mail după validarea expeditorilor legitimi

RESPONSABIL

Responsabil e-mail

DOVADA FINALIZĂRII

Politică aprobată și livrare legitimă reușită

Testați recuperarea clienților față de informații personale reutilizate

RESPONSABIL

Fraudă și relații cu clienții

DOVADA FINALIZĂRII

Rezultat și excepții corectate

Cereți verificare independentă pentru schimbări sensibile de beneficiar

RESPONSABIL

Trezorerie și plăți

DOVADA FINALIZĂRII

Procedură aprobată și cerere testată

Eliminați datele personale reale inutile din testare

RESPONSABIL

Inginerie și protecția datelor

DOVADA FINALIZĂRII

Acceptarea responsabilului și verificarea accesului

Verificați expunerea camerelor, controlerelor și accesul furnizorilor

RESPONSABIL

Operațiuni și infrastructură

DOVADA FINALIZĂRII

Configurație aprobată și alarme verificate

3Zilele 61–90

Restabiliți un flux esențial cu copii protejate și autentificări separate

RESPONSABIL

Responsabil serviciu și infrastructură

DOVADA FINALIZĂRII

Timp, integritate și acceptarea fluxului

Exersați notificarea furnizorului și delimitarea datelor personale

RESPONSABIL

Achiziții, protecția datelor și coordonator

DOVADA FINALIZĂRII

Cronologie și dovezi ale deciziilor

Exersați raportarea cibernetică, de date și financiară aplicabilă

RESPONSABIL
Juridic și responsabili raportare

DOVADA FINALIZĂRII
Destinatari, termene și rezervă în afara programului

Exersați o întrerupere împreună cu o afirmație publică de acces sau date

RESPONSABIL
CISO, comunicare și responsabili afaceri

DOVADA FINALIZĂRII
Decizii separate pentru servicii, identitate și divulgare

Raportați conducerii dovezile neclarificate și controalele întârziate

RESPONSABIL
CISO și sponsor executiv

DOVADA FINALIZĂRII
Indicatori acceptați, responsabili și decizii datate

12.2 Responsabilitatea pe roluri

CISO răspunde de prioritizare și escaladare. Responsabilul de afaceri acceptă serviciul minim și recuperarea. Identitatea verifică conturile și sesiunile. Achizițiile și responsabilii datelor stabilesc sfera furnizorilor. Protecția datelor și juridicul decid aplicabilitatea și notificarea. Relațiile cu clienții gestionează comunicarea sigură.

SOC și infrastructura trebuie să identifice dovada care închide întrebarea tehnică. Resetarea parolei nu demonstrează revocarea fiecărei sesiuni sau permisiuni delegate. Pagina accesibilă nu demonstrează recuperarea fluxului de afaceri. Tăcerea autorului nu dovedește lipsa copierii.

12.3 Indicatori de finalizare

Măsură	Țintă	Dovadă
Livrarea alertelor	Funcțională până în ziua 30	Test rutat reușit
Semnal nou de cont sau acces	Responsabil numit și decizie consemnată	Verificarea contului și sesiunii
Căi critice de administrare	Responsabile și testate până în ziua 60	Verificarea MFA și privilegiilor
Schimbări sensibile de plată	Verificate independent până în ziua 60	Procedură aprobată și exercițiu
Recuperarea fluxului esențial	Demonstrată până în ziua 90	Acceptare de afaceri și timp consemnat
Rute de raportare aplicabile	Exersate până în ziua 90	Cronologie, destinatari și rezervă
Dovezi materiale neclarificate	Vizibile conducerii până în ziua 90	Responsabil, motiv și următoarea decizie

Tratați exercițiul nereușit drept dovadă pentru o corecție datată. Nu declarați testul incomplet reușit doar pentru că există o procedură sau a avut loc o întâlnire.

12.4 Cum poate ajuta Brandefense

Brandefense oferă informații despre amenințări, monitorizare a mediului clandestin și capacități privind suprafața de atac. Folosiți constatările pentru a defini domeniile, mărcile, conturile și serviciile de monitorizat, apoi legați alertele relevante de responsabili. Vizibilitatea produselor completează verificarea locală și dovezile incidentului. [S19]

Solicitați o demonstrație Brandefense despre expunerea identității, informațiile ransomware și serviciile pe care echipa trebuie să le protejeze.

CONCLUZII PRINCIPALE

01

Atribuiți fiecărei priorități un responsabil de afaceri și dovezi observabile.

02

Testați împreună notificarea furnizorilor, verificarea plăților și recuperarea independentă.

03

Închideți acțiunile prin decizii demonstrate și servicii funcționale.

ANEXE

Anexe

A–E

ÎNTREBAREA ACESTUI CAPITOL

Ce populații, date și limite de încredere guvernează raportul?

4

tipuri de dovezi păstrate separat

Anexa A. Sferă și limitele dovezilor 128

Anexa B. Registrul dovezilor 131

Anexa C. Surse 133

Anexa D. Glosar 138

Anexa E. Alte constatări oficiale și context de campanie 140

Anexa A. Sferă și limitele dovezilor

Țările de comparație au fost selectate ca exemple doar pentru a oferi context; alegerea lor nu implică un clasament sau o evaluare politică.

A.1 Obiectul cercetării

Raportul acoperă România, 1 ianuarie–22 noiembrie 2026, după data postării. Capătul solicitat este sfârșitul zilei de 22 noiembrie în UTC. Cercetarea a avut loc înaintea încheierii zilei, deci materialul publicat ulterior poate lipsi.

Comunicările publice sunt datate după publicare, cu păstrarea separată a datei incidentului sau detectării când este disponibilă. Intervalul recent este 8–22 noiembrie. Un eveniment mai vechi este inclus ca dezvăluire recentă fără mutarea sa în noiembrie.

Cititorii vizați sunt conducerea securității, operațiunile, responsabilii identității și infrastructurii, echipele financiare și de protecție a clienților, precum și juridicul și comunicarea. Deciziile privesc verificarea, limitarea, recuperarea, notificarea și prevenirea efectelor secundare.

A.2 Postări și anunțuri

Brandefense Blackhole furnizează dovezile postărilor păstrate. Raportul distinge populația etichetată cu țara de arhiva păstrată și setul de 256 de postări de forum etichetate. Perspectivele au acoperiri diferite și nu sunt prezentate ca populații incluse una în alta. [S1]

Arhiva conține 41.379 postări distincte. Populația etichetată cu țara este 773.764. O postare poate fi anunț, răspuns, relatare, catalog sau incident pretins. Aceste obiecte nu pot fi adunate ca atacuri independente.

Referințele la țară și limbile nu stabilesc vizarea, naționalitatea, coordonarea de către un stat sau victimele. Volumul pretins nu stabilește persoane unice. Data pretinsă nu stabilește obținerea sau accesul inițial. Fragmentele autentice rămân afirmații ale sursei, cu aceeași incertitudine ca dosarul.

Raportul nu stabilește o tranzacție infracțională încheiată doar dintr-un preț sau răspuns vizibil. Textul similar nu stabilește același set de date, furtul inițial, un operator comun sau transferul dintre vânzători.

Observațiile domeniilor selectate formează o populație separată și nu se adaugă totalurilor de publicare de mai sus. Referirea la un domeniu corporativ global nu stabilește singură un eveniment în România. [S1][S2]

A.3 Domenii selectate și observații privind expunerea

Portofoliul conține 250 de domenii candidate, selectate pentru importanța instituțională și sectorială. Independența, proprietatea completă și sfera exclusiv românească nu sunt stabilite pentru fiecare candidat. [S2]

Rezultatele descriu domeniile selectate, nu prevalența națională sau un clasament oficial. Domeniile de grup și globale pot servi mai multe entități sau populații. Observațiile pasive își păstrează numitorii evaluați și rezultatele necunoscute.

Atlas furnizează valoarea națională de 50/100 (B) pentru portofoliul selectat de 250 de domenii. 79 de domenii aveau date de autentificare oferite la vânzare. Se publică numai evaluarea națională; tabelele sectoriale conțin numărul anonim al semnalelor. Nu se publică evaluări Atlas sectoriale ori de grup. [S2]

Observațiile expunerii și controalelor pasive sunt datate 22 noiembrie 2026. Numerele dispozitivelor sunt observații minime; evidențele de autentificare pot fi istorice, iar populațiile se suprapun. Observațiile cardurilor cu etichete financiare nu verifică statutul emitentului sau sursa expunerii cardurilor.

A.4 Materiale privind cardurile

Cifrele acoperă numai cardurile apărute în clar în postările clandestine păstrate. Brandefense detectează carduri furate prin multe alte metode, în afara raportului. Observațiile nu măsoară furtul național, valabilitatea curentă sau pierderile din fraudă. [S4]

Emitenții, țările, postările și cardurile sunt unități diferite. Nu trebuie combinate cu asocieri de dispozitive sau autentificări. Valabilitatea tranzacției și măsurile pentru clienți cer dovezi specifice emitentului.

A.5 Înregistrări ransomware

Ransompedia furnizează populația înregistrărilor pentru România și cei patru comparatori. Datele descriu publicarea, nu începutul intruziunii. Înregistrarea este o afirmație infracțională și poate privi o organizație repetată sau o structură de grup. [S3]

Intervalul 2026 și întregul an 2025 au durate inegale. Economiile, practicile de comunicare și vizibilitatea diferite împiedică un clasament al riscului sau o rată de creștere pentru perioade egale.

Aceeași etichetă în mai multe țări nu stabilește un operator comun pentru fiecare eveniment. Eticheta fluxului nu atribuie independent un incident oficial fără o relație concretă.

A.6 Vulnerabilități și cercetare tehnică

Raportul verifică CVE-2023-50224 în NVD și avertizarea producătorului. Exemplele hardware și de versiuni corectate păstrează limitele regionale și de versiune. Nu stabilesc vulnerabilitatea folosită împotriva unei anumite organizații românești. [S11][S12]

Matricea Cereal selectează tehnici din documentul citat. Este context descriptiv, nu regulă de detecție testată sau dovada fiecărei tehnici în România. Nu sunt incluse cod ofensiv funcțional ori detalii de acces ale victimelor. [S8]

A.7 Incidente publice și limitele acoperirii

Comunicările oficiale, constatările autorităților, investigațiile originale și relatările atribuite susțin cazurile publice. Relatarea oficială poate fi preliminară ori poate păstra neclarități despre date. Declarațiile citate sunt identificate când originalul nu a putut fi verificat.

Raportul include atacuri externe, abuz de acces, erori de prelucrare, posibile incidente operaționale și context de aplicare a legii. Rămân distincte. Cele 31 de dosare bazate pe relatări oficiale nu înseamnă 31 de intruziuni confirmate produse în 2026.

Unele perioade din arhive și comunicări originale nu au putut fi verificate. Acoperirea este limitată la materialul citat și nu este un inventar național exhaustiv. Sursele inaccesibile nu fundamentează afirmații de absență.

O organizație afectată este numită doar când confirmarea oficială și relatările mai largi susțin numele. Alte cazuri folosesc roluri generice. Legăturile către articole identificatoare sunt omise. Dacă sursa este chiar organizația nenumită, adresa ei este de asemenea omisă.

A.8 Încredere și neutralitate

Încredere ridicată privește o afirmație susținută direct de dovezi sau relatare clară. Nu autentifică fiecare afirmație dintr-un anunț. **Încredere moderată** indică o interpretare cu alternative semnificative neclarificate. **Neverificat** păstrează afirmația fără a-i adopta conținutul.

Atribuirile către state sunt evaluările surselor. Nu se deduce atribuirea din limbă, etichetă de țară, naționalitate sau slogan. Raportul nu adoptă poziții despre guverne, alegeri, partide, relații externe sau teritorii.

Scenariile condiționale sunt ipoteze de planificare. Valoarea lor constă într-un responsabil și un declanșator observabil, nu într-o probabilitate numerică pretinsă.

Anexa B. Registrul dovezilor

Fișele reproduc fragmente autentice scurte, cu detaliile victimelor și contactele eliminate. Traducerile păstrează limita afirmației. ID-urile fișelor sunt referințe publice, nu identificatori ai înregistrărilor brute.

Fișă	Dată	Mediu	Pseudonim	Limbă	Capitol
B01	2026-01-01	Forum	renquix	EN	4
B02	2026-01-21	Forum	EchoEcho	EN	4
B03	2026-02-16	Forum	Reddington66	EN	4
B04	2026-03-04	Forum	Eliphas	EN	4
B05	2026-04-02	Forum	xorcat	EN	4
B06	2026-04-07	Forum	xorcat	EN	4
B07	2026-03-20	Forum	fent888	EN	4
B08	2026-04-24	Forum	johnapp	EN	4
B09	2026-05-07	Forum	moxzey	EN	4
B10	2026-05-24	Forum	somewhere	EN	4
B11	2026-06-20	Forum	tempp991	EN	4
B12	2026-11-10	Forum	ternny	EN	4
B13	2026-11-10	Forum	NorthDivision	EN	4
B14	2026-03-11	Telegram	313 Team	AR	6
B15	2026-03-17	Telegram	DDoSia Project	RU	6
B16	2026-03-17	Telegram	DDoSia Project	EN	6
B17	2026-10-30	Telegram	RBL Leviathan Ghost	EN	6
B18	2026-07-28	Telegram	BD Anonymous	EN	6
B19	2026-08-01	Telegram	NoName-labelled account	EN	6
B20	2026-09-12	Telegram	ServerKillers-labelled relay	EN	6
B21	2026-04-07	Telegram	Access-claim account	RU	6
B22	2026-07-30	Telegram	NoName-labelled account	EN	6

Fișă	Dată	Mediu	Pseudonim	Limbă	Capitol
B23	2026-07-31	Telegram	NoName-labelled account	EN	6
B24	2026-09-04	Telegram	Escanors Marketplace	EN	4

Manifestul cazurilor conține 14 dosare de anunțuri și 31 de dosare bazate pe relatări oficiale. Cazurile pot grupa actualizări și afirmații conexe. Totalul de 45 este editorial, nu atacuri, victime sau intruziuni confirmate unice din 2026.

Anexa C. Surse

Referințele de date proprii descriu dovezile păstrate de Brandefense. Paginile editorului nu reproduc independent cifrele. Sursele externe au fost citite pentru afirmațiile folosite; legăturile omise păstrează limita numirii publice.

S1: Odin by Brandefense · Dovezi din postări și observații agregate pentru România · sursă · Verificat la 2026-11-22.

S2: Odin by Brandefense · Evaluarea națională Atlas, expunerea domeniilor selectate și observații pasive · sursă · Verificat la 2026-11-22.

S3: Ransompedia · Observații privind înregistrările ransomware din România și regiune · sursă · Verificat la 2026-11-22.

S4: Brandefense Blackhole · Date agregate despre carduri de plată în postările păstrate · sursă · Verificat la 2026-11-22.

S5: DataReportal · Digital 2027: România; date din octombrie 2026 · sursă · Verificat la 2026-11-22.

S6: ESET · Exchange la micul dejun: cercetare despre Cereal · sursă · Verificat la 2026-11-22.

S7: SRI · Declarație privind răspunsul la incidentul e-mailului guvernamental, 11 noiembrie 2026 · sursă · Verificat la 2026-11-22.

S8: ESET · Studiu tehnic despre Cereal, 10 noiembrie 2026 · sursă · Verificat la 2026-11-22.

S9: SRI · Declarație privind participarea la operațiunea Masquerade, 8 aprilie 2026 · sursă · Verificat la 2026-11-22.

S10: FBI și parteneri internaționali · Aviz privind manipularea DNS pe routere, 7 aprilie 2026 · sursă · Verificat la 2026-11-22.

S11: NVD · Înregistrarea CVE-2023-50224 · sursă · Verificat la 2026-11-22.

S12: TP-Link · Aviz privind hardware-ul și firmware-ul pentru CVE-2023-50224 · sursă · Verificat la 2026-11-22.

S13: Monitorul Oficial prin EUR-Lex · Ordonanța de urgență 155/2024, textul oficial inițial · sursă · Verificat la 2026-11-22.

S14: Senatul României · Legea promulgată 124/2025 de aprobare cu modificări a Ordonanței 155/2024 · sursă · Verificat la 2026-11-22.

S15: ANSPDCP · Întrebări frecvente oficiale: notificarea încălcării securității datelor personale · sursă · Verificat la 2026-11-22.

S18: RFC Editor · RFC 9989: DMARC · sursă · Verificat la 2026-11-23.

S19: Brandefense · Demonstrație de produs și capabilități · sursă · Verificat la 2026-11-22.

S20: Sursă publică oficială sau atribuită · Raportare CONPET privind incidentul sistemelor informatice de afaceri · sursă · Verificat la 2026-11-22.

S21: Sursă publică oficială sau atribuită · Actualizare guvernamentală privind incidentul ransomware din administrarea cadastrală · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S22: Sursă publică oficială sau atribuită · Anunț privind aplicația de achiziții pentru finanțări publice · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S23: Sursă publică oficială sau atribuită · Comunicat privind incidentul ransomware din administrația penitenciară · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S24: Sursă publică oficială sau atribuită · Actualizare privind restabilirea serviciilor administrației penitenciare în ziua următoare · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S25: Sursă publică oficială sau atribuită · Declarație DNSC privind disponibilitatea site-ului · sursă · Verificat la 2026-11-22.

S26: Sursă publică oficială sau atribuită · Comunicat privind aplicația auxiliară din piața de capital · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S27: Sursă publică oficială sau atribuită · Declarații ale operatorului de comunicații și DNSC privind incidentul · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S28: Sursă publică oficială sau atribuită · Avertizare DNSC privind frauda prin două apeluri cu identitate falsă · sursă · Verificat la 2026-11-22.

S29: Sursă publică oficială sau atribuită · Studiul poliției privind fraudele de investiții din ianuarie până în septembrie · sursă · Verificat la 2026-11-22.

S30: Sursă publică oficială sau atribuită · Investigația poliției privind frauda cu conturi pe o platformă comercială · sursă · Verificat la 2026-11-22.

S31: SRI · Avertizare SRI privind falsificarea identității apelantului · sursă · Verificat la 2026-11-22.

S32: Sursă publică oficială sau atribuită · Avertizare a poliției privind vishingul · sursă · Verificat la 2026-11-22.

S33: ANSPDCP · Decizie ANSPDCP privind ransomware într-o unitate turistică · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S34: ANSPDCP · Decizie ANSPDCP privind securitatea într-o firmă de servicii petroliere · sursă · adresa articolului este omisă · Verificat la 2026-11-23.

S35: ANSPDCP · Decizie ANSPDCP privind securitatea la un furnizor de credit · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S36: ANSPDCP · Decizie ANSPDCP privind un server de testare software · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S37: ANSPDCP · Decizie ANSPDCP privind phishingul asupra unui administrator · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S38: ANSPDCP · Decizie ANSPDCP privind aplicații de telecomunicații · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S39: ANSPDCP · Decizie ANSPDCP privind procesarea notificărilor bancare · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S40: ANSPDCP · Decizie ANSPDCP privind accesul intern neautorizat într-o bancă · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S41: ANSPDCP · Decizie ANSPDCP privind drepturile de acces într-o bancă · sursă · adresa articolului este omisă · Verificat la 2026-11-23.

S42: ANSPDCP · Decizie ANSPDCP privind validarea conturilor în comerț · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S43: ANSPDCP · Decizie ANSPDCP privind o aplicație auto administrată de furnizor · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S44: ANSPDCP · Decizie ANSPDCP privind securitatea în servicii profesionale · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S45: ANSPDCP · Decizie ANSPDCP privind securitatea într-o firmă de servicii industriale · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S46: ANSPDCP · Decizie ANSPDCP privind servicii comerciale transfrontaliere · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S47: ANSPDCP · Decizie ANSPDCP privind o aplicație din turism · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S48: ANSPDCP · Decizie ANSPDCP privind controlul accesului în producție · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S49: ANSPDCP · Decizie ANSPDCP privind securitatea într-o firmă de produse de consum · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S50: ANSPDCP · Decizie ANSPDCP privind securitatea serviciilor pentru clienți · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S51: ANSPDCP · Decizie ANSPDCP privind un cont de administrator în comerț · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S52: Sursă publică oficială sau atribuită · Actualizare a poliției privind frauda transfrontalieră pe o platformă fiscală · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S53: Sursă publică oficială sau atribuită · Relatare privind investigația DIICOT asupra phishingului cu conturi sociale · sursă · Verificat la 2026-11-22.

S54: Sursă publică oficială sau atribuită · Relatare privind avertizarea DNSC despre fraude cu pretexte de curierat · sursă · Verificat la 2026-11-22.

S55: Sursă publică oficială sau atribuită · Relatare privind avertizarea DNSC despre phishing cu identități instituționale false · sursă · Verificat la 2026-11-22.

S56: Sursă publică oficială sau atribuită · Relatare privind avertizarea DNSC despre phishing cu taxe pentru mărci · sursă · Verificat la 2026-11-22.

S57: ASF · Registrul ASF de alerte pentru investitori · sursă · Verificat la 2026-11-22.

S58: ANSPDCP · Arhiva completă de știri ANSPDCP · sursă · Verificat la 2026-11-22.

S59: Sursă publică oficială sau atribuită · Prim-viceguvernatorul BNR despre stresul cibernetic și transmiterea efectelor asupra lichidității · sursă · Verificat la 2026-11-22.

S60: ASF · Prezentarea oficială ASF despre DORA · sursă · Verificat la 2026-11-22.

S61: Sursă publică oficială sau atribuită · Autoritatea regională anunță oficial restabilirea aplicației de achiziții · sursă · Verificat la 2026-11-22.

S62: Sursă publică oficială sau atribuită · Declarația oficială a ministerului de externe privind DDoS · sursă · Verificat la 2026-11-22.

S63: Sursă publică oficială sau atribuită · Relatare a radioului național privind un posibil incident cu regulatoare frigorifice, potrivit DNSC · sursă · Verificat la 2026-11-22.

S64: Sursă publică oficială sau atribuită · Relatare națională privind declarația despre malware pe un site fiscal municipal · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S65: Sursă publică oficială sau atribuită · Anunțul unui operator de salubritate privind incidentul portalului pentru clienți · Adresa sursei este omisă pentru protejarea organizației · Verificat la 2026-11-22.

S66: Sursă publică oficială sau atribuită · Operatorul de salubritate restabilește portalul · Adresa sursei este omisă pentru protejarea organizației · Verificat la 2026-11-22.

S67: ASF · Regulamentul delegat 2025/301, copie oficială ASF · sursă · Verificat la 2026-11-23.

S68: Sursă publică oficială sau atribuită · Relatarea inițială privind imagini de supraveghere expuse public · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S69: Sursă publică oficială sau atribuită · Răspunsul autorității pentru protecția copilului la întrebările privind expunerea · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S71: Sursă publică oficială sau atribuită · Ministerul spaniol de interne confirmă operațiunea LeakBase și participarea României · sursă · Verificat la 2026-11-22.

S72: Sursă publică oficială sau atribuită · Parchetul din Paris confirmă operațiunea SocksEscort și participarea României · sursă · Verificat la 2026-11-22.

S73: Reuters prin Investing.com · Investigație Reuters privind accesul raportat la e-mail militar, text republicat · sursă · Adresa articolului este omisă. Textul republicat sub semnătura Reuters a fost citit; domeniul original este indisponibil · Verificat la 2026-11-22.

S74: Sursă publică oficială sau atribuită · Răspunsul instituției militare la relatările publice privind e-mailul · sursă · Adresa articolului este omisă; răspuns oficial citat de radioul național · Verificat la 2026-11-22.

S75: Sursă publică oficială sau atribuită · Copie publicată de presă a anexei preliminare DNSC din 22 iulie 2026 · sursă. Constatări preliminare; publicare fără autorizarea DNSC; nu este raportul final (S115) · Statutul publicării verificat la 2026-11-23.

S76: Sursă publică oficială sau atribuită · Declarație oficială inițială privind incidentul din administrarea cadastrală · sursă · Verificat la 2026-11-22.

S77: Sursă publică oficială sau atribuită · Declarație DNSC privind ransomware într-o bancă, citată în relatarea financiară inițială · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S78: Sursă publică oficială sau atribuită · Relatare națională independentă privind răspunsul la ransomware într-o bancă · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S79: Sursă publică oficială sau atribuită · Incidentul site-ului unei facultăți, confirmat într-un interviu cu decanul · sursă · adresa articolului este omisă · Verificat la 2026-11-22.

S80: Sursă publică oficială sau atribuită · Actualizarea unei firme de servicii de investiții confirmă accesul la baza de date pentru deschiderea conturilor · sursă · Verificat la 2026-11-23.

S81: Sursă publică oficială sau atribuită · DNSC explică temperaturile anormale din șase magazine românești · sursă · Verificat la 2026-11-22.

S82: Sursă publică oficială sau atribuită · Notificarea unei librării către clienți privind perturbarea de securitate · sursă · Verificat la 2026-11-22.

S83: Sursă publică oficială sau atribuită · Redeschiderea librăriei confirmată prin e-mail către clienți · sursă · Verificat la 2026-11-22.

S84: Sursă publică oficială sau atribuită · Declarația conducerii unei universități privind perturbarea infrastructurii · sursă · Verificat la 2026-11-22.

S85: Sursă publică oficială sau atribuită · Răspuns guvernamental privind identificatorii personali din documente publicate · sursă · Verificat la 2026-11-22.

S86: Sursă publică oficială sau atribuită · Actualizarea unui grup comercial privind activitatea malițioasă în rețea și restabilirea serviciilor · Adresa sursei este omisă pentru protejarea organizației · Verificat la 2026-11-22.

S87: Sursă publică oficială sau atribuită · Directorul fiscal municipal prezintă consiliului atacuri repetate · sursă · Verificat la 2026-11-22.

S88: Sursă publică oficială sau atribuită · Verificări preliminare ale poliției după întreruperi ale site-urilor municipale · sursă · Verificat la 2026-11-22.

S89: Sursă publică oficială sau atribuită · Declarație municipală privind indisponibilitatea plăților online · sursă · Verificat la 2026-11-22.

S90: Sursă publică oficială sau atribuită · Municipalitatea anunță înlocuirea planificată a sistemului de plată · Adresa sursei este omisă pentru protejarea organizației · Verificat la 2026-11-22.

S91: Sursă publică oficială sau atribuită · Autoritatea fiscală avertizează privind apeluri cu identități false de inspectori · sursă · Verificat la 2026-11-22.

S92: Sursă publică oficială sau atribuită · Autoritatea fiscală regională reia avertizarea privind vishingul · sursă · Verificat la 2026-11-22.

S93: Sursă publică oficială sau atribuită · Autoritatea de reglementare poștală avertizează privind momeli cu colete și WhatsApp · sursă · Verificat la 2026-11-22.

S95: Sursă publică oficială sau atribuită · Poliția neagă explicația unui atac cibernetic pentru retragerea radarelor · sursă · Verificat la 2026-11-22.

S96: Sursă publică oficială sau atribuită · Relatare independentă privind întreruperea înrolării clienților unei firme de servicii de investiții · sursă · Verificat la 2026-11-23.

S97: Sursă publică oficială sau atribuită · Relatarea locală inițială reproduce declarația universității · sursă · Verificat la 2026-11-22.

S98: Sursă publică oficială sau atribuită · Relatare oficială din sectorul transporturilor privind atacuri repetate asupra site-ului · sursă · Verificat la 2026-11-22.

S99: Sursă publică oficială sau atribuită · Fondatorul platformei pentru flote descrie un DDoS anterior și răspunsul · sursă · Verificat la 2026-11-22.

S100: Sursă publică oficială sau atribuită · Studiu de caz al furnizorului privind incidentul de disponibilitate al platformei pentru flote · Adresa sursei este omisă pentru protejarea organizației · Verificat la 2026-11-22.

S101: Sursă publică oficială sau atribuită · Autoritatea pentru digitalizare avertizează privind SMS-uri cu o platformă de plată clonată · sursă · Verificat la 2026-11-22.

S102: Sursă publică oficială sau atribuită · Furnizorul de energie avertizează privind phishingul cu facturi · Adresa sursei este omisă pentru protejarea organizației · Verificat la 2026-11-22.

S103: Sursă publică oficială sau atribuită · O redacție primește e-mailuri care imită identitatea unei bănci · sursă · Verificat la 2026-11-22.

S104: Sursă publică oficială sau atribuită · Momeală de rambursare trimisă de cititori, destinată cumpărătorilor online · sursă · Verificat la 2026-11-22.

S106: Sursă publică oficială sau atribuită · Relatarea din raportul anual privind deturnarea unei plăți la un producător din apărare · sursă · Verificat la 2026-11-22.

S111: Sursă publică oficială sau atribuită · Înregistrare NVD privind ocolirea unei funcții de securitate Office · sursă · Verificat la 2026-11-22.

S112: Sursă publică oficială sau atribuită · Actualizarea de securitate Microsoft Office 2016 MSI KB5002713 · sursă · Actualizare specifică ediției; nu se aplică pentru Click-to-Run · Verificat la 2026-11-23.

S113: Sursă publică oficială sau atribuită · Buletinul cibernetic CERT-EU pentru februarie 2026, publicat la 2 martie · sursă · Sinteza Neusploit prezintă cercetarea Zscaler · Verificat la 2026-11-22.

S114: Sursă publică oficială sau atribuită · Cercetare Insikt Group privind BlueDelta și HOOKEDGE · sursă · Sunt păstrate atribuirea sursei și limitele perioadei de activitate · Verificat la 2026-11-23.

S115: DNSC prin AGERPRES · Precizări DNSC privind publicarea anexei preliminare, 2 septembrie 2026 · sursă · Anexă preliminară, nu un raport final autorizat · Verificat la 2026-11-23.

S116: Programul CVE / Microsoft · Înregistrarea CVE privind produsele Office afectate și limitele versiunilor · sursă · Verificat la 2026-11-23.

S117: Microsoft · Versiuni de securitate Office care includ remedierea CVE-2026-21509 · sursă · Verificat la 2026-11-23.

S118: Microsoft · Recomandări de securitate MSRC din ianuarie 2026 pentru CVE-2026-21509 · sursă · Verificat la 2026-11-23.

S119: Microsoft · Istoricul actualizărilor pentru Office 2016 C2R și Office 2019 · sursă · Verificat la 2026-11-23.

Anexa D. Glosar

Termen	Explicație simplă
Anunț de acces	Afirmație că un cont sau serviciu poate fi accesat; nu stabilește acces funcțional
Evidență de autentificare	Înregistrare asociată datelor de autentificare; nu neapărat cont curent sau parolă validă
Asociere de dispozitiv	Relație observată între dispozitiv și domeniu; proprietatea și infectarea curentă cer verificare
Combolist	Colecție de identificatori de cont și parole, posibil din mai multe surse vechi
CRM	Gestionarea relațiilor cu clienții: sisteme pentru interacțiuni și înregistrări comerciale
CSIRT	Echipă care coordonează răspunsul la incidente cibernetice
DDoS	Refuz distribuit de serviciu: activitate care urmărește indisponibilitatea prin trafic sau consumul resurselor
DKIM	DomainKeys Identified Mail: semnarea e-mailului pe baza domeniului
DMARC	Aliniere a autentificării e-mailului, raportare și tratament solicitat mesajelor [S18]
DNSSEC	Extensii pentru autentificarea datelor DNS; observarea delegării nu este validare completă
DORA	Cadrul UE pentru reziliența operațională digitală în sectorul financiar [S60]
HSTS	HTTP Strict Transport Security: politică web care cere browserului utilizarea HTTPS
TIC	Tehnologia informației și comunicațiilor
KYC	Cunoașterea clientelei: procese de verificare a identității și clientului
MFA	Autentificare multifactor: folosirea mai multor factori distincți
NIS2	Directiva UE de securitate cibernetică reflectată în cadrele naționale
Phishing	Comunicare înșelătoare pentru obținerea informațiilor, accesului sau unei acțiuni neautorizate
Înregistrare ransomware	Publicare infracțională care numește o presupusă victimă; distinctă de confirmarea criptării ori furtului

Termen	Explicație simplă
RTO	Obiectiv de timp de recuperare: întreruperea maximă permisă de planul de afaceri
SCADA	Sisteme pentru supravegherea, achiziția datelor și controlul proceselor industriale
Router SOHO	Router de rețea pentru un birou mic sau locuință [S10]
SPF	Sender Policy Framework: autorizarea publicată a gazdelor expediatoare
TLS	Transport Layer Security: protecția conexiunii, nu dovada securității punctului final
Vishing	Phishing prin telefon sau alt canal de voce

Anexa E. Alte constatări oficiale și context de campanie

Intrările suplimentare păstrează lecții distincte. Datele sunt de publicare. O sancțiune poate descrie un incident mai vechi, iar unele constatări nu stabilesc un autor extern.

Publicat	Constatarea sursei	Limita clasificării	Implicație defensivă
13 ianuarie	Incident al unei aplicații turistice; investigație încheiată în 2025 [S47]	Publicarea nu stabilește un atac din 2026	Verificați accesul și garanțiile procesatorului
19 ianuarie	Foaie internă cu date medicale ale angajaților distribuită cu protecție insuficientă [S48]	Fără atac extern sau dată de eveniment din 2026 stabilite	Restricționați circulația datelor sensibile ale personalului
4 februarie	Slăbiciune de autentificare și resetare a expus un director de angajați din UE [S46]	Investigație încheiată în decembrie 2025	Testați recuperarea și sfera populației
25 martie	Atac asupra unei aplicații auto administrate de furnizor; date publicate [S43]	Publicarea nu stabilește un atac din 2026	Verificați furnizorul și accesul la dovezi
3 aprilie	Atac IT la servicii profesionale, cu afectarea confidențialității și disponibilității [S44]	Fără incident comun stabilit cu decizii similare	Desemnați responsabilul monitorizării accesului
30 aprilie	Atac la servicii industriale, cu date ale personalului și corespondenților expuse [S45]	Momentul și legăturile rămân neclarificate	Examinați fluxurile și evidențele accesului
18 iunie	Validare slabă în aplicația mobilă, cu facturi și livrări ale altei persoane vizibile [S42]	Deficiență de autorizare; fără autor extern stabilit	Testați autorizarea pe înregistrări și notificarea
28 august	Atac la produse de consum, afectând identitatea și contactele [S49]	Data atacului neprecizată	Verificați monitorizarea și jurnalele protejate
2 octombrie	Constatare la servicii pentru clienți cu date de personal, salarizare și bancare [S50]	Data atacului neprecizată	Includeți personalul și furnizorii în evaluare
30 octombrie	Atac asupra contului administrativ al unui comerciant, cu identificatori și autentificări interne expuse [S51]	Data atacului neprecizată	Protejați administrarea și examinați sesiunile
Noiembrie	Angajat bancar a depășit accesul autorizat la datele clienților [S41]	Constatare internă, nu campanie externă comună	Verificați scopul profesional și excepțiile

Indexul ANSPDCP include și alte comunicări de conformitate, procedură sau activitate instituțională. Nu sunt toate incidente cibernetice. Cele 54 de comunicări nu trebuie transformate într-un total național de atacuri. [S58]

În martie, relatări oficiale ale autorităților străine identifică participarea României la operațiuni privind LeakBase și SocksEscort. Sunt observații de aplicare internațională a legii. Nu stabilesc totaluri românești de victime sau dispozitive și nu se combină numitori globali diferiți. [S71][S72]

O comunicare din 4 mai despre un serviciu pentru flote descrie DDoS din toamna lui 2025. Furnizorul precizează că o componentă distinctă a rămas operațională. Este context despre o comunicare istorică și limitele serviciilor, nu un atac nou din 2026 sau un număr de vehicule afectate. [S99][S100]

O relatare din august care citează raportul anual DNSC pentru 2025 descrie un incident la un producător, cu e-mail și redirecționarea plăților. Aparține anului anterior. Susține verificarea independentă a instrucțiunilor de plată modificate, fără a intra în numărul evenimentelor produse în anul curent. [S106]

Despre raport

Odin by Brandefense a pregătit pachetul de cercetare cu asistență AI. Combină observații din date proprii cu relatări publice în limitele surselor. Ediția engleză este principală; ediția română include notificarea traducerii AI și păstrează cifrele, ID-urile și directivele.

Raportul aparține seriei Brandefense Country Report · Romania 2026. Nu estimează prevalența națională, nu autentifică anunțuri infracționale și nu atribuie independent activitate unor state. Scopul este legarea dovezilor susținute de decizii de securitate cu responsabili.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO