ANCOM
Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii

Str. Delea Nouă nr.2, Sector 3, 030925 Bucureşti, România
Telefon: 0372 845 400 / 0372 845 454. Fax: 0372 845 402
E-mail: ancom@ancom.org.ro. Website: www.ancom.org.ro

GHID DE RAPORTARE A INCIDENTELOR CU IMPACT SEMNIFICATIV ASUPRA FURNIZĂRII REŢELELOR ŞI SERVICIILOR DE COMUNICAŢII ELECTRONICE

Cuprins

1. INTRODUCERE

Rețelele publice de comunicații electronice și serviciile de comunicații electronice destinate publicului răspund nevoilor fundamentale de comunicare și de informare a persoanelor având totodată și rolul de infrastructură suport pentru un număr în creștere de tehnologii și aplicații.

Serviciile de comunicații electronice joacă un rol foarte important în viața de zi cu zi a utilizatorilor. Activitățile utilizatorilor privați, cât și ale celor din mediul de afaceri se bazează pe buna funcționare a rețelelor şi serviciilor de comunicații electronice a căror importanță este accentuată în momentul în care acestea devin indisponibile. Totodată și alte sectoare ale economiei naționale se bazează pe infrastructura de comunicații, iar breșele de securitate și pierderea integrității rețelelor de comunicații pot afecta aceste sectoare într-un mod semnificativ. Prin urmare, incidentele care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice pot avea un impact negativ semnificativ pentru furnizorii și utilizatorii acestora, de natură să afecteze și alte sectoare ale economiei naționale.

1.1. Cadru legal

Ordonanța de Urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată cu modificări și completări prin Legea nr. 140/2012, cu modificările și completările ulterioare, include un capitol special dedicat securității şi integrității rețelelor şi serviciilor de comunicații electronice care transpune în legislația națională prevederile Capitolului IIIa din *Directiva 2002/21/CE a Parlamentului European și a Consiliului privind un cadru de reglementare comun pentru rețelele şi serviciile de comunicaţii electronice, astfel cum a fost revizuită prin Directiva 2009/140/CE a Parlamentului European și a Consiliului*, şi are ca scop stabilirea unui cadru general pentru asigurarea utilizării în siguranță a rețelelor şi serviciilor de comunicații electronice, în special prin informarea utilizatorilor în legătură cu incidentele care afectează în mod semnificativ securitatea şi integritatea rețelelor şi serviciilor, precum şi prin stabilirea responsabilităților furnizorilor şi a atribuțiilor autorității de reglementare în acest domeniu.

Conform art. 47 din Ordonanța de Urgență a Guvernului nr. 111/2011:

„(1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a notifica ANCOM, în cel mai scurt timp, cu privire la orice încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra furnizării rețelelor sau serviciilor.

(2) ANCOM poate informa publicul cu privire la existența cazului prevăzut la alin. (1) sau poate solicita furnizorului să informeze publicul cu privire la existenta acestui caz, atunci când consideră că este în interesul public."

Astfel, furnizorii au obligația de a transmite Autorității Naționale pentru Administrare și Reglementare în Comunicații (ANCOM), în cel mai scurt timp, informații cu privire la încălcarea securității sau pierderea integrității care are un impact semnificativ asupra furnizării rețelelor sau serviciilor de comunicații electronice. Totodată, art. 48 din Ordonanța de Urgență a Guvernului nr. 111/2011 prevede dreptul ANCOM de a stabili modalitatea de implementare a dispozițiilor art. 47. În aceste condiții, prin *Decizia președintelui ANCOM nr. 512/2013 privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului şi raportarea incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice* a fost stabilită, printre altele, și procedura de raportare a incidentelor cu impact semnificativ asupra furnizării rețelelor şi serviciilor de comunicaţii electronice, inclusiv prin determinarea circumstanțelor, a formatului notificărilor şi condițiilor aplicabile în cazul cerințelor de notificare.

1.2. Schema de raportare

O procedură națională eficace de raportare oferă numeroase beneficii. Un astfel de sistem facilitează informarea, în timp util, a părților interesate în legătură cu producerea unui incident. În același timp, ANCOM poate urmări eficiența măsurilor de securitate adoptate de furnizori, precum şi a răspunsului acestora în momentul producerii incidentelor, poate colecta date referitoare la tipurile de amenințări şi vulnerabilități ce vor fi utilizate în cadrul unei analize aprofundate a securității rețelelor şi serviciilor, constituind o bază pentru emiterea de recomandări și ghiduri de bune practici.

Datele privind incidentele sunt fundamentale pentru dezvoltarea unei înțelegeri clare a naturii şi amplorii provocărilor existente la adresa securității şi integrității rețelelor şi serviciilor.

În cazul incidentelor cu impact semnificativ, ANCOM poate analiza în detaliu cauzele incidentului, acțiunile furnizorului de rețele publice de comunicații electronice sau de servicii de comunicații electronice şi alte aspecte relevante legate de acest incident. Prin analizarea incidentelor cu impact semnificativ, ANCOM poate evalua nivelul de securitate al rețelelor şi serviciilor de comunicații electronice şi eficacitatea măsurilor de reglementare implementate. ANCOM poate cere furnizorilor și totodată, pe baza informațiilor colectate, îi poate îndruma astfel încât aceștia să ia măsuri corespunzătoare pentru evitarea producerii pe viitor a acelui incident/tip de incident. Analizele statistice ale incidentelor pot constitui, de asemenea, un instrument eficient în vederea urmării și monitorizării tendințelor și evoluției în timp a securității și integrității rețelelor și serviciilor.

Pe lângă o definire clară a domeniului de aplicare şi a obiectivelor de raportare, în spatele fiecărui sistem de raportare trebuie să existe o reprezentare clară a incidentelor ce trebuie raportate. Există patru elemente cheie pentru un sistem de raportare eficient:

- definirea clară a categoriilor cauzelor incidentului (motivul pentru care incidentul a avut loc);
- formatul de raportare, ale cărui câmpuri/domenii trebuie să fie bine definite;
- criteriile și parametrii luați în considerate pentru a raporta/defini un incident;
- valorile pragurilor acestor criterii și parametri care declanșează mecanismul de raportare.

În scopul colectării cât mai facile, complete și într-un format comparabil a informațiilor necesare în notificarea finală privind incidentele raportate, ANCOM a implementat o aplicație online de raportare disponibilă din pagina web proprie. Mai multe detalii privind aplicația se găsesc la punctul 6 din prezentul Ghid.

În figura 1 este reprezentată schema de raportare a incidentelor către ANCOM.

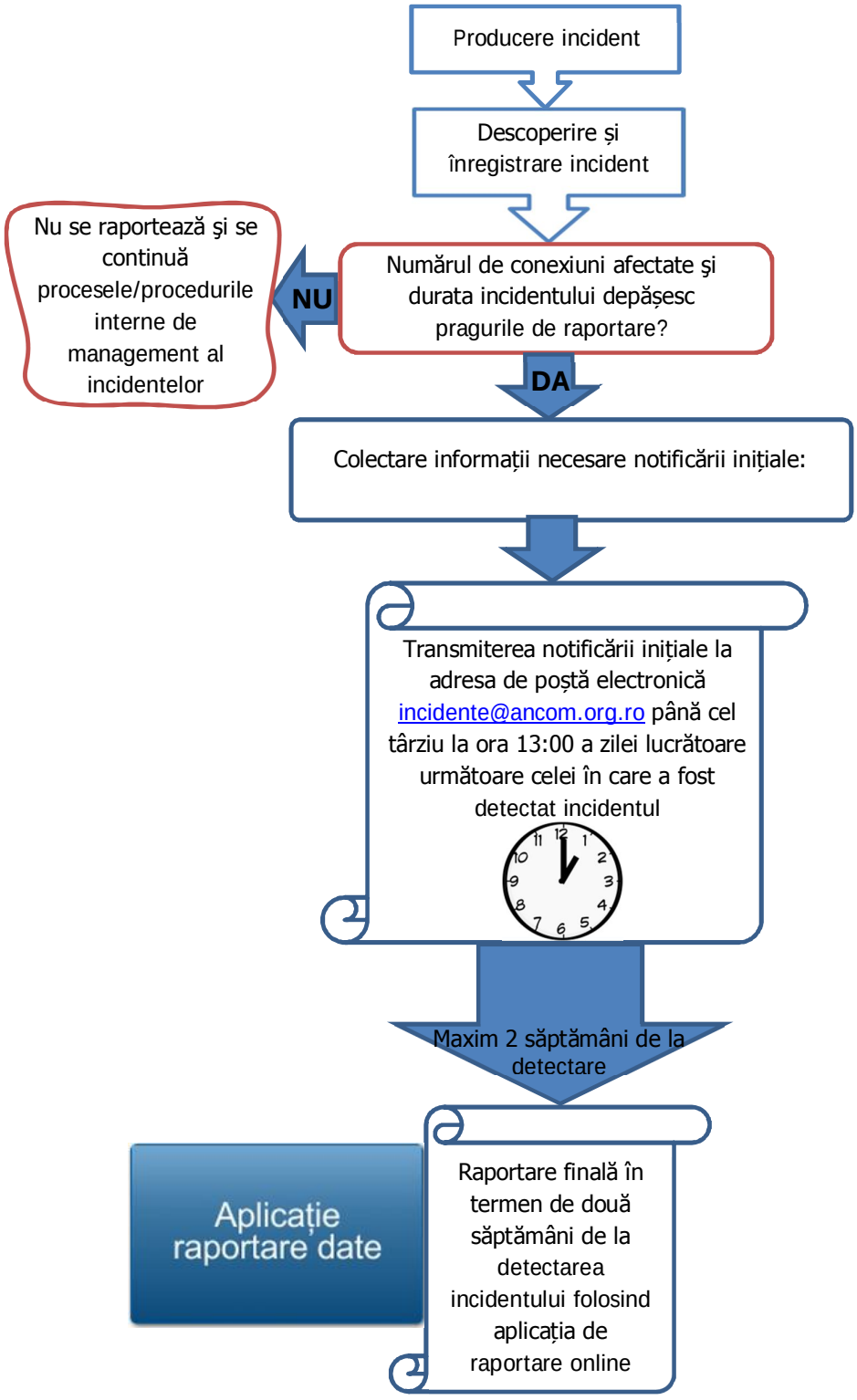

Fig. 1 Schema de raportare

1.3. Scop şi obiectiv

Obiectivul principal al Ghidului este de a clarifica anumite aspecte privind mecanismul de raportare a incidentelor cu impact semnificativ asupra securității şi integrității rețelelor şi serviciilor de comunicații electronice, stabilit prin Decizia președintelui ANCOM nr. 512/2013, cu **scopul** de a primi informații complete, corecte şi comparabile asupra respectivelor incidente.

Prezentul Ghid se adresează furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului care au obligația de a raporta către ANCOM incidentele cu impact semnificativ asupra securității şi integrității rețelelor şi serviciilor de comunicații electronice conform Deciziei președintelui ANCOM nr. 512/2013.

1.4. Definiții[1]

Securitatea şi integritatea rețelelor şi serviciilor de comunicații electronice – capacitatea unei rețele sau a unui serviciu de comunicații electronice de a rezista evenimentelor, accidentale sau rău intenționate, care pot compromite sau afecta continuitatea furnizării rețelelor şi serviciilor la un nivel de performanță echivalent cu cel anterior producerii evenimentului;

Incident – un eveniment care poate afecta sau amenința, direct ori indirect, securitatea şi integritatea rețelelor şi serviciilor de comunicații electronice;

Incident cu impact semnificativ – acel incident care afectează un număr mai mare de 5.000 de conexiuni, timp de cel puțin 60 de minute;

Măsuri de securitate – mijloace (de natură administrativă, managerială, tehnică sau juridică) de management al riscurilor, incluzând politici, acțiuni, planuri, echipamente, facilități, proceduri, tehnici etc. menite să elimine ori să reducă riscurile privind securitatea şi integritatea rețelelor sau a serviciilor de comunicații electronice.

2. NOTIFICAREA INIŢIALĂ

Notificarea inițială reprezintă un raport cu privire la faptul că un incident cu impact semnificativ a avut loc. Acesta trebuie să fie transmis până cel târziu la ora 13:00 a zilei lucrătoare următoare celei în care a fost detectat incidentul, prin e-mail, la adresa incidente@ancom.org.ro. Notificarea conține caracteristicile de bază ale incidentului şi estimarea consecințelor acestuia, pe baza informațiilor disponibile imediat după eveniment.

Astfel, în primă fază, furnizorul va trebui să raporteze doar informații minime referitoare la un incident:

- Data și ora descoperirii incidentului; Se vor transmite data și ora descoperirii incidentului și se va menționa dacă aceasta coincide cu data și ora de producere a incidentului;
- Serviciile și/sau rețelele care sunt afectate de incident; Se vor transmite toate serviciile afectate sau posibil afectate de incident;
- Estimarea ariei geografice afectate se va face prin menționarea județului și în funcție de informațiile deținute la momentul respectiv, prin menționarea localității/localităților, a sectorului, daca este cazul, sau a procentajului afectat dintr-un județ sau regiune;
- Estimarea numărului de conexiuni afectate se va face în funcție de informațiile deținute la momentul respectiv;

[1] Definițiile sunt conform Deciziei președintelui ANCOM nr. 512/2013.

- Estimarea efectelor incidentului asupra furnizării rețelelor şi serviciilor de către alți furnizori, pe piața națională de comunicații electronice sau pe cea din alt stat membru al Uniunii Europene;
- Estimarea efectelor în ceea ce privește apelarea numărului unic pentru apeluri de urgență 112;
- O descriere sumară a cauzei/cauzelor care a/au provocat incidentul prin menționarea cauzei, a categoriei cauzei și a modului prin care aceasta a afectat rețelele și serviciile de comunicații electronice (spre exemplu, ninsori abundente/fenomen natural au condus la ruperea cablului de fibră optică, furtul firelor de cupru/acțiune rău intenționată prin secționarea cablului de cupru, întrerupere alimentare cu energie electrică/cauză externă/parte terță ce a cauzat nefuncționarea unei stații de bază etc.);
- Estimarea graficului de restabilire a furnizării rețelelor şi serviciilor de comunicații electronice în parametrii normali de funcționare se va face prin transmiterea acțiunilor ce sunt planificate a se realiza și estimarea momentului în care acestea vor fi realizate, inclusiv estimarea momentului în care încetează efectul incidentului;
- Îndrumările oferite de furnizor utilizatorilor în vederea minimizării efectelor incidentului, dacă este cazul;
- Informațiile oferite publicului cu privire la existența unui incident, modalitatea de comunicare şi ora la care au fost comunicate informațiile, dacă este cazul;
- Alte aspecte/elemente care pot permite ANCOM să decidă dacă informarea publicului privind incidentul este sau nu în interesul publicului;
- Datele de contact (nume, prenume, număr de telefon, număr de fax, adresă de poștă electronică) ale persoanei/persoanelor care poate/pot da mai multe informații privind incidentul.

În cazul în care un astfel de incident poate afecta furnizarea rețelelor şi serviciilor de comunicații electronice de către un furnizor din alt stat membru al Uniunii Europene, ANCOM va avea în vedere informarea autorității de reglementare din respectivul stat şi ENISA[2] cu privire la acest incident.

În același timp, în cazul în care un incident petrecut într-un alt stat membru al Uniunii Europene afectează sau poate afecta furnizarea rețelelor şi serviciilor de comunicații electronice de către unul sau mai mulți furnizori din România, după primirea informării din partea autorității de reglementare din acel stat membru UE, ANCOM va avea în vedere informarea respectivului sau a respectivilor furnizori.

În situația în care furnizorul deține toate informațiile necesare notificării finale în termenul în care trebuia să transmită notificarea inițială, acesta poate să completeze direct formularul aferent notificării finale prin intermediul aplicației online cu condiția de a se încadra cu raportarea finală în termenul în care trebuia să transmită notificarea inițială.

3. NOTIFICAREA FINALĂ

Notificarea finală va trebui să conțină informații complete cu privire la incidentul cu impact semnificativ asupra furnizării rețelelor şi serviciilor de comunicații electronice, precum şi un rezumat al măsurilor luate pentru a elimina vulnerabilitățile identificate şi pentru a preveni reapariția incidentului în viitor. Este necesar ca furnizorii să aloce resurse umane care să se ocupe de managementul incidentelor și de raportarea acestora.

Transmiterea notificării finale trebuie realizată în termen de două săptămâni de la detectarea incidentului folosind aplicația de raportare online.

[2] ENISA - the European Union Agency for Network and Information Security

În anumite cazuri, este posibil ca furnizorii să nu dețină la momentul transmiterii notificării finale toate informațiile privind incidentul care a afectat securitatea şi integritatea rețelelor şi serviciilor de comunicații electronice. În acest caz, furnizorii trebuie să transmită în două săptămâni de la detectarea incidentului notificarea finală cu toate informațiile disponibile la acel moment, menționând explicit faptul că urmează să transmită informații suplimentare, urmând ca, în momentul în care dețin şi celelalte informații, să le transmită ANCOM printr-o notificare suplimentară, însă nu mai târziu de 3 săptămâni de la detectarea incidentului cu impact semnificativ.

Începând cu data de 1 ianuarie 2014, transmiterea notificării finale şi după caz, a celei suplimentare se realizează exclusiv prin intermediul unei aplicații disponibile pe pagina de internet a ANCOM, ca înscris în formă electronică, căruia i s-a încorporat, atașat sau i s-a asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat nesuspendat sau nerevocat la momentul respectiv şi generată cu ajutorul unui dispozitiv securizat de creare a semnăturii electronice.

Obiectivul formatului standardizat de raportare a incidentelor este ca ANCOM să se asigure că informațiile transmise de furnizori sunt comparabile. Utilizarea unui model standard face ca procesul de colectare şi analiză a datelor să fie mai eficient şi, în același timp, asigură coerență fluxului de informații transmise.

3.1 Pragurile de raportare

Un incident trebuie raportat către ANCOM de fiecare dată când impactul incidentului este egal sau mai mare decât un prag predefinit. Impactul unui incident este cuantificat in primă fază din punctul de vedere a doi parametri: numărul total de conexiuni afectate, respectiv durata incidentului. Astfel, mecanismul de raportare către ANCOM este declanșat în momentul în care un incident afectează un număr total mai mare de 5.000 de conexiuni timp de cel puțin 60 de minute.

Conform Deciziei președintelui ANCOM nr. 512/2013, o conexiune reprezintă:

- în cazul serviciilor de acces la internet la puncte fixe: o conexiune de acces la internet; un abonat poate avea alocate mai multe conexiuni; în acest caz vor fi incluse în numărătoare toate conexiunile afectate, alocate acelui abonat;

- în cazul serviciilor de transmisiuni de date la puncte fixe: o conexiune de acces la servicii de transmisiuni de date; un abonat poate avea alocate mai multe conexiuni; în acest caz vor fi incluse în numărătoare toate conexiunile afectate, alocate acelui abonat;

- în cazul serviciilor de telefonie la punct fix: o linie telefonică alocată unui abonat de către un furnizor prin intermediul propriei rețele publice fixe pe care o operează sau prin rețeaua publică fixă a unui terț; un abonat poate avea alocate mai multe linii telefonice; în acest caz vor fi incluse în numărătoare toate liniile telefonice afectate alocate acelui abonat;

- în cazul serviciilor de telefonie, acces la internet şi transmisiuni de date furnizate prin intermediul rețelelor radio mobile terestre: o cartelă SIM activă[3];

- în cazul serviciilor de retransmisie a programelor media audiovizuale liniare: o conexiune de retransmisie a programelor media audiovizuale; un abonat poate avea alocate

[3] O cartelă SIM activă este considerată orice cartelă SIM pe bază de abonament, respectiv orice cartelă SIM preplătită utilizată în mod efectiv cel puțin o dată, în sensul că a fost efectuat/recepționat un apel sau a fost trimis un SMS/MMS ori de pe care au fost utilizate servicii de transmisiuni de date cel puțin o dată în perioada de raportare determinată în baza Deciziei președintelui Autorității Naționale pentru Administrare şi Reglementare în Comunicații nr. 333/2013 privind raportarea unor date statistice de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului.

mai multe conexiuni; în acest caz vor fi incluse în numărătoare toate conexiunile afectate, alocate acelui abonat.

Acest criteriu este pur cantitativ şi nu ia în considerare tipul utilizatorilor afectați. Astfel, fiecare utilizator are aceeași importanță şi nu există nicio distincție, de exemplu, între un utilizator persoană fizică şi o bancă sau un spital. Nivelul de importanță al unei infrastructuri deservite de către un furnizor este analizat din perspectiva identificării și protejării infrastructurilor critice, conform legislației primare specifice.

În cadrul aplicației de raportare se va/vor bifa serviciul/serviciile afectate de incident și se va specifica pentru fiecare serviciu în parte numărul de conexiuni afectate.

3.1.1 Metodologia de estimare a numărului de conexiuni afectate pentru serviciile furnizate prin intermediul unor rețele publice mobile terestre[4]

În cazul serviciilor furnizate prin intermediul unor rețele publice mobile terestre, furnizorul va estima numărul de conexiuni afectate. Metoda de estimare a numărului de cartele SIM afectate de un incident este prezentată mai jos.

În momentul apariției unui incident se identifică celulele afectate.

Traficul total pierdut la nivelul tuturor celulelor afectate ($T_{pierdut}$), pe fiecare serviciu (voce, internet şi date), se consideră a fi traficul înregistrat în săptămâna anterioară, în același interval de timp în care a avut loc incidentul (ziua și intervalul orar), la nivelul acelor celule.

Traficul total înregistrat la nivelul rețelei (T_{retea}) se consideră a fi suma traficului din toate celulele din rețea în intervalul de timp respectiv (ziua și intervalul orar) din săptămâna anterioară producerii incidentului.

Numărul de cartele SIM afectate se calculează astfel:

$$N_{cartele\ SIM\ afectate} = N_{ds} \frac{T_{pierdut}}{T_{retea}}$$

N_{ds} reprezintă numărul de cartele SIM active pe respectivul serviciu la nivelul furnizorului, conform raportării în baza Deciziei președintelui Autorității Naționale pentru Administrare şi Reglementare în Comunicații nr. 333/2013 privind raportarea unor date statistice de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului.

În calculul traficului total pierdut se are în vedere atât traficul originat, cât şi traficul terminat la nivelul celulelor afectate. Algoritmul propus se va aplica tuturor tipurilor de servicii la puncte mobile.

3.2 Parametrii de impact raportați

3.2.1 Numărul total de conexiuni afectate de incident

Acest parametru indică impactul cantitativ global al incidentului din punctul de vedere al conexiunilor afectate. Numărul total de conexiuni afectate trebuie să fie mai mare de 5.000 pentru ca incidentul să se încadreze pentru raportare și reprezintă suma tuturor conexiunilor afectate pe fiecare tip de serviciu.

Exemplu de caz în care un incident depășește pragurile de raportare:

Dacă un incident afectează 3.001 de conexiuni la serviciul de telefonie fixă și 2.000 de conexiuni la serviciul de acces la internet la puncte fixe, numărul total de conexiuni afectate va fi 5.001 de conexiuni, caz în care parametrul număr total de conexiuni este mai are decât

[4] Metodologia de estimare se regăsește detaliată și în Decizia președintelui ANCOM nr. 512/2013.

pragul de 5.000 și dacă se depășește și pragul de 60 de minute al parametrului "Durată", atunci incidentul trebuie raportat.

3.2.2 Resursele/echipamentele afectate de incident

Resursele ce pot fi afectate de incidente vizează în principiu echipamente/componente/sisteme (hardware/software) din rețeaua de comunicații electronice a furnizorului care prin afectarea lor conduc la întreruperea serviciului de comunicații electronice.

În scopul colectării unor informații comparabile privind resursele afectate de incidente, raportarea acestora se va face după cele 3 criterii, detaliate în subcapitolele de mai jos.

O descriere succintă a abrevierilor se poate găsi în Anexa 1 a prezentului ghid.

3.2.2.1 Identificarea resursei afectate

Raportarea tipului resursei se va face prin alegerea categoriei de resurse de mai jos și specificarea concretă a tipului de echipament/echipamente afectat/e și a numărului acestora, dacă sunt afectate mai multe echipamente de același tip, separat pe fiecare tip de echipament.

Echipamentele trecute în parantezele fiecărei categorii de mai jos sunt trecute cu titlu de exemplu și nu constituie o listă exhaustivă de echipamente pentru fiecare categorie.

1. Stații de bază și controlere mobile (BTS, BSC, NodeB, eNodeB, RNC, MME, ANDSF, PCRF);
2. Centre de comutație în rețele mobile (MSC, SGSN, GGSN, PGW, SGW, ePDG sau similar);
3. Regiștrii de localizare în rețele mobile (HLR, VLR, HSS, AuC sau similar);
4. Centre de mesagerie mobilă (SMSC, MMSC);
5. Routere și switch-uri IP (DSLAM, BRAS, Metro router, Metro switch, router, switch, EDGE router, IP PBX, Core router sau similar);
6. Echipamente din noduri de transmisiune (echipamente de modulație/demodulație, echipamente de multiplexare/demultiplexare pe tehnologie SDH, PDH, DWDM, sau similar);
7. Centre de comutație în rețele fixe (Centrală locală/de tranzit/națională/internațională, soft switch, server de gestiune a abonaților);
8. Puncte de interconectare (IXP, POI etc);
9. Servere de adresare (DHCP, DNS);
10. Sisteme de securitate (IDS, IPS, AAA, LDAP, VPN, firewall etc);
11. Platforma de taxare;
12. Componente/Platforme de servicii (IPTV, VoIP, IMS, STP, SCP etc);
13. OSS (Operations Support Systems) și BSS (Business Support Systems);
14. Sisteme de retenție a datelor și interceptare legală a comunicațiilor;
15. Centre de retransmisie de programe media audiovizuale liniare (head-end);
16. Echipamente din rețeaua de distribuție a serviciilor de retransmisie de programe media audiovizuale liniare (amplificatoare, distribuitoare, etc);
17. Medii de transmisiune: cabluri (cablu torsadat, cablu coaxial, cablu fibră optică etc.), radio (link-uri radio, microunde etc.);
18. Alte resurse (specificați).

Observații

1. Categoria Medii de transmisiune prin unde radio va fi bifată la resurse afectate doar în cazurile în care echipamentul care generează linkul radio este perfect funcțional dar intervin interferențe pe linia de transmisiune, spre exemplu construcția unei clădiri care blochează vizibilitatea între cele două puncte conectate prin linkul radio.
   Dacă se produce o defecțiune fizică sau logică a unui echipament care generează un link radio sau mai multe linkuri radio, atunci se va considera la Resurse afectate categoria în care se află acel echipament, deoarece linkul radio este afectat din cauza defectării echipamentului care l-a generat (spre exemplu dacă este afectat un link radio datorită defectării multiplexorului pe tehnologie SDH care generează acel link, se va bifa categoria Echipamente din noduri de transmisiune).

2. În cazul nefuncționării/defectării unui/unor echipament/e cauzată de întreruperea alimentării principale/de backup (redresoare, baterii etc.) cu energie electrică sau cauzată de nefuncționarea unui echipament de monitorizare/control al temperaturii (aer condiționat, cooler etc.), se vor bifa și specifica echipamentul/echipamentele nefuncționale chiar dacă acestea nu sunt defectate și se va specifica faptul că acestea au fost afectate la nivel suport.

3.2.2.2 Localizarea resursei în cadrul rețelei

După locul pe care îl ocupă în arhitectura rețelei, resursa afectată poate fi localizată astfel:

a) Interconectare – legătura fizică și logică realizată între rețele publice de comunicații electronice care permite comunicarea dintre utilizatorii rețelelor sau accesul la servicii; serviciile pot fi furnizate de către părțile implicate sau de către terțe părți care au acces la rețeaua respectivă; interconectarea este o formă specifică de acces realizată de operatorii de rețele publice de comunicații (de exemplu IXP-ul se află în această categorie);

b) Rețea centrală (Core network) – este centrul rețelei care furnizează servicii utilizatorilor conectați la aceasta prin rețeaua de acces.

c) Rețea de acces (Acces network) – cuprinde accesul individual al utilizatorilor la rețelele și serviciile de comunicații electronice (de exemplu stațiile de bază se află în această categorie).

3.2.2.3 Clasificarea modului în care a fost afectată resursa

Resursele pot fi afectate fizic/hardware, logic/software sau datorită întreruperii furnizării unor servicii auxiliare (ex. lipsei alimentării cu energie electrică). Astfel, s-au identificat 3 niveluri posibile la care pot fi afectate resursele:

a) Nivel logic – face referire la componentele software ale echipamentelor.

b) Nivel fizic – face referire la componentele hardware ale echipamentelor.

c) Nivel suport – face referire la componentele suport ale echipamentelor precum cele utilizate pentru alimentarea cu energie electrică, echipamente auxiliare (de alimentare de backup cu energie electrică - Grup electrogen, baterie/UPS, Sisteme de monitorizare și control al temperaturii - cooler, aer condiționat etc.), instalații electrice (cabluri electrice, siguranțe, întrerupătoare, transformatoare etc. deținute de furnizor) etc..

Exemple de completare a câmpurilor aferente resurselor afectate:

Dacă se întrerupe furnizarea cu energie electrică a două BTS iar grupul electrogen care trebuia să preia alimentarea stațiilor cu energie electrică se defectează, cele 4 câmpuri incluse în aplicație, aferente resurselor afectate se vor completa după cum urmează:

- *se va bifa categoria resursei afectate, în acest caz "Stații de bază și controlere mobile",*
- *se va/vor specifica apoi concret resursele afectate, în cazul acesta "2 BTS",*
- *se va bifa nivelul la care este afectată resursa, în acest caz nivelul suport,*
- *se va bifa partea de rețea din care face parte resursa afectată, în cazul acesta "Rețeaua de acces".*

În cazul în care o întreagă stație de bază ar fi afectată din cauza defectării unui echipament component al stației de bază, categoria resursei afectate va fi tot "Stații de bază și controlere mobile" după care se va specifica "1 BTS", se vor bifa "nivelul fizic" și "Rețeaua de acces" apoi în câmpul Detalierea cauzei se va preciza concret echipamentul defectat care a condus la afectarea întregii stații de bază.

3.2.3 Durata incidentului

Durata incidentului reprezintă intervalul de timp, exprimat în minute, din momentul în care serviciul începe să se degradeze sau s-a întrerupt (data și ora producerii incidentului), până în momentul în care acesta este adus în parametrii normali de funcționare.

În cazul în care nu se cunoaște și nu se poate afla momentul în care serviciul începe să se degradeze sau s-a întrerupt și se cunoaște doar momentul (data și ora) descoperirii incidentului, atunci se va specifica acest lucru și durata incidentului se va calcula ca interval de timp, exprimat în minute, din momentul descoperirii incidentului până în momentul în care acesta este adus în parametrii normali de funcționare.

3.2.4 Aria/răspândirea geografică

Aria/răspândirea geografică se referă la zona de impact a incidentului. Dacă se produce un incident major o întreagă regiune poate fi afectată. Impactul poate fi diferit, în funcție de aria sau răspândirea geografică și de densitatea populației, de exemplu. Aferent acestui parametru există în cadrul aplicației 3 câmpuri. Primul câmp va fi completat cu numărul de județe afectate, cel de al doilea câmp va cuprinde numele județelor afectate, iar cel de al treilea câmp va cuprinde, în funcție de disponibilitatea informațiilor, date de localizare mai precise (ex. localitate, sector, cartier).

3.2.5 Impactul asupra apelurilor de urgență

Se consideră că există un impact asupra apelurilor de urgență dacă utilizatorii nu pot apela numărul de urgență, din motive ce țin de afectarea funcționării rețelei operatorului în cauză.

În cazul rețelelor mobile, dacă apelurile de urgență nu pot fi realizate prin rețeaua proprie atunci se consideră impact asupra apelurilor de urgență, prin urmare, câmpul "Impactul asupra apelurilor de urgență" se va completa și în acest caz cu "Da" indiferent dacă în zona afectată de incident este sau nu posibil roamingul național.

3.3 Descrierea incidentului

Prin descrierea incidentului se dorește detalierea succesiunii evenimentelor, pentru a putea avea o imagine detaliată și de ansamblu a ceea ce s-a întâmplat.

Exemplu de completare a câmpului:

Datorită vântului puternic, un cablu de fibră optică s-a rupt întrerupând furnizarea serviciilor de acces la internet la puncte fixe.

3.4 Tipul și detalierea cauzei

Cauza unui incident reprezintă evenimentul sau factorul care declanșează incidentul. ANCOM a identificat 5 cauze ale incidentelor care afectează securitatea şi integritatea rețelelor şi serviciilor de comunicații electronice: eroare umană, eroare de sistem, fenomen natural, acțiune rău intenționată şi cauză externă/parte terță.

3.4.1 Cauzele unui incident

3.4.1.1 Eroare umană

În categoria eroare umană trebuie încadrate incidentele cauzate de operarea şi configurarea defectuoasă a echipamentelor, sistemelor, utilităților, implementarea şi folosirea greșită a instrumentelor software, aplicarea eronată a procedurilor etc.

În această categorie sunt incluse incidente cauzate de erori umane ale personalului intern.

- Configurare sau dezvoltare și operare defectuoasă a:
  - Echipamentelor de rețea,
  - Platformelor,
  - Aplicațiilor (software),
  - Copiilor de rezervă,
  - Bazelor de date etc..
- Aplicarea eronată a procedurilor:
  - Proceduri de management al configurărilor,
  - Proceduri de management al schimbărilor,
  - Proceduri de management al controlului accesului şi al identităților,
  - Proceduri de management al incidentelor etc..

Exemplu de incident de securitate cauzat de erori umane:

- *Un angajat aplică în mod eronat procedura de mentenanță a echipamentelor de răcire, ceea ce conduce la defectarea unui echipament pentru controlul temperaturii. Astfel, supraîncălzirea și afectarea echipamentelor pe care le deservea conduc la întreruperea serviciului de acces la internet prin conexiuni permanente la punct fix.*

3.4.1.2 Eroare de sistem

În categoria eroare de sistem sunt incluse incidentele datorate defecțiunilor hardware, erorilor de programare ale software-lui din vina producătorului aplicației, dimensionării şi/sau implementării greșite a rețelei şi erorilor în elaborarea politicilor, procedurilor sau manualelor etc..

Exemplu de incident de securitate cauzat de erori de sistem:

- *Un bug software la platforma SMS întrerupe furnizarea serviciului de mesagerie scurtă.*

3.4.1.3 **Fenomen natural**

Categoria fenomen natural include incidente cauzate de dezastre şi fenomene naturale, cum ar fi:

- Condiții meteorologice nefavorabile (ex. ninsori abundente, furtuni, temperaturi excesive, tornade, etc.)
- Cutremure,
- Tsunami,
- Pandemii,
- Inundații,
- Incendii,
- Alunecări de teren,
- Erupții vulcanice,
- Fenomene meteorologice spațiale etc.

Exemplu de incident de securitate cauzat de fenomene naturale:

- *Ninsorile abundente cauzează întreruperea furnizării energiei electrice în zonă întrerupând astfel retransmisia serviciilor de programe media audiovizuale liniare terestre cu acces la punct fix tip CATV.*

3.4.1.4 **Acțiune rău intenționată**

Categoria acțiune rău intenționată va include incidentele cauzate de acțiunile efectuate în mod deliberat, ca de exemplu: acces neautorizat la echipamente de rețea, platforme, aplicații (software), baze de date, atacuri de tip DoS sau DDoS, efectuare de modificări neautorizate ale sistemelor şi datelor, vandalism, sabotaj, furt etc., și care se soldează cu afectarea funcționării anumitor resurse.

Acest tip de atac presupune ca o persoană sau un program să primească acces logic sau fizic, fără permisiune, la o rețea, un sistem, o aplicație, date sau alte resurse ale furnizorului. O astfel de încălcare a securității poate fi rezultatul unui atac planificat, şi poate proveni dintr-o amenințare internă ori externă.

Cauzele incluse în această categorie pot fi împărțite în două subcategorii: „Atacuri asupra securității logice" şi „Atacuri asupra securității fizice".

1. Exemple de atacuri asupra securității logice sunt redate mai jos:
   - Acces logic neautorizat la:
     - Echipamente de rețea,
     - Platforme,
     - Aplicaţii (software),
     - Copii de rezervă,
     - Baze de date,
     - Date confidențiale (date de identificare, de configurare, date de trafic şi de localizare, informații despre clienți etc.)
   - Utilizarea neautorizată a unor privilegii (extinderea privilegiilor către un utilizator extern, extinderea privilegiilor unui utilizator intern, furtul de identitate, atacuri de tip „social engineering" etc.);

- Pierderea de date ce afectează securitatea rețelei, a infrastructurii sau a sistemelor;
- Modificarea datelor sau fișierelor critice de sistem sau a serviciilor de date;
- Modificarea comenzilor de securitate;
- Login-uri ostile în sistemele informatice ale furnizorilor;
- Re-rutarea sau întreruperea rutării traficului (ex. alterarea tabelelor de rutare a traficului din rețea);
- Răspândirea de malware în sistemele informatice ale furnizorilor (ex. viruși de calculator, programe de instalare de tip „back-door", troieni, programe de monitorizare ce afectează sistemul de operare etc.);
- Atacuri de blocare a serviciului (DoS sau DDoS);
- Creșterea bruscă a traficului (spam, atacuri centralizate etc.);
- Exploatarea vulnerabilităților software şi hardware.

2. Exemple de atacuri asupra securității fizice sunt redate mai jos:
   - Acces fizic neautorizat:
     - Accesarea hardware-ului sistemului şi modificarea neautorizată a acestuia;
     - Pătrunderea fizică în amplasamentele sistemelor informatice.
   - Furtul oricăror tipuri de echipamente, cabluri etc.

Exemple de incidente de securitate cauzate de acțiuni rău intenționate:

- *Un atac de tip brute force prin care atacatorul a accesat un echipament de management al conexiunilor din rețeaua centrală mobilă și realizează trafic nelegitim, conduce la blocarea intenționată de către furnizor a conexiunilor respective pentru perioada de răspuns la incident cu scopul de a opri traficul nelegitim pe acele conexiuni. (acțiune rău intenționată asupra securității logice).*
- *Furtul cablurilor de cupru ale unui furnizor de comunicații electronice cauzează întreruperea serviciului de telefonie furnizat prin rețele publice fixe sau cu mobilitate limitată (acțiune rău intenționată asupra securității fizice).*

3.4.1.5 Cauză externă/parte terță şi corelarea cu alte cauze

Nu toate acțiunile (sau inacțiunile) care pot provoca un incident se datorează furnizorului de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului şi sunt sub controlul direct al acestuia. Astfel, există şi incidente provocate de părți terțe, precum: distrugerea unor echipamente şi cabluri în urma unor lucrări de construcție, defecțiuni în rețeaua de distribuție a energiei electrice etc.

Cauza externă trebuie corelată cu una din celelalte 4 cauze: eroare umană, eroare de sistem, fenomen natural sau acțiune rău intenționată. În cazul excepțional în care nu se cunosc suficiente informații care să permită corelarea cauzei externe cu una din celelalte 4 cauze, se va bifa doar cauza externă/parte terță.

Exemplu de incident din categoria cauză externă/parte terță în corelare cu altă cauză:

- *Un cablu este secționat datorită operațiilor de excavare din zonă, ce cauzează întreruperea serviciului de acces la internet prin conexiuni permanente la punct fix.(cauză externă corelată cu eroare umană).*

3.5 Mai multe informații despre cauza incidentului

Câmpul „Detalierea cauzei" trebuie să descrie succesiunea evenimentelor care au condus la producerea incidentului.

De cele mai multe ori, bifarea tipului cauzei incidentului nu clarifică cauza incidentului. Spre exemplu, indicarea cauzei externe corelată cu acțiune rău intenționată nu lămurește dacă incidentul a fost cauzat de un furt sau de acte de vandalism/sabotaj.

Exemplu de completare a câmpului:

Ninsorile abundente au produs un incident la furnizorul de energie electrică, întrerupând alimentarea cu energie electrică a două stații de bază care nu erau prevăzute cu sisteme de alimentare de urgență de tip back-up.

4. ALTE INFORMAȚII DESPRE INCIDENT

a) *Acțiuni de răspuns la incident (inclusiv momentul când au fost luate)*

Tratarea unui incident presupune mai multe etape: identificarea incidentului şi a consecințelor acestuia, limitarea consecințelor incidentului, eliminarea cauzei şi prevenirea reapariției acesteia, revenirea la un mod normal de furnizare a serviciilor, evaluarea modului de acțiune al organizației şi eficienței în procesul de tratare a consecințelor acestui incident şi nu în ultimul rând, analiza experienței dobândite cu această ocazie astfel încât eventualele erori evidențiate să nu se mai repete.

În cadrul acestui câmp se va prezenta graficul acțiunilor luate, specificând ora la care a fost realizată fiecare acțiune. Un exemplu de completare al acestui câmp se găsește mai jos la pct. 5 „Exemple de incidente și completarea câmpurilor de raportare".

b) *Măsurile luate sau planificate pentru a împiedica producerea unui incident similar*

Organizația trebuie să își extindă mijloacele de acțiune și prin măsuri pro active de analizare a potențialelor amenințări şi riscuri, astfel încât să prevină apariția incidentelor.

Furnizorii de rețele şi servicii de comunicații electronice trebuie să dezvolte procese care să trateze și să răspundă la incidente, dar şi procese care să prevină apariția sau reapariția incidentelor. Acestea includ procese pentru planificarea şi implementarea unui management al incidentelor, îmbunătățirea securității infrastructurii organizației pentru a preveni incidentele sau pentru a atenua efectele unui incident, detectarea, trierea şi răspunsul la incidente atunci când acestea apar.

Măsurile de securitate au ca obiective principale reducerea semnificativă a numărului de incidente şi întreruperi operaționale, a fraudelor, prevenirea pierderii, distrugerii, furtului sau compromiterii resurselor, îmbunătățirea calității serviciilor oferite utilizatorilor, creșterea încrederii utilizatorilor în serviciile oferite de furnizor.

Măsurile de securitate sunt dedicate protecției resurselor (hardware, software, informații etc.), constituind practici/metode prin care vulnerabilitățile şi amenințările se elimină sau se previn, se descoperă şi se raportează în scopul acțiunilor corective, minimizându-se efectele negative pe care le pot produce.

Un exemplu de completare al acestui câmp se găsește în continuare.

5. EXEMPLE DE INCIDENTE ȘI COMPLETAREA CÂMPURILOR DE RAPORTARE

Se recomandă furnizorilor ca raportările incidentelor cu impact semnificativ să cuprindă informații cât mai complete și detaliate pentru fiecare câmp în parte pentru evitarea schimbului

de corespondență cu scopul clarificării informațiilor corespunzătoare unui incident. De aceea, prezentăm mai jos două exemple de incidente și nivelul de detaliu ce trebuie atins în completarea raportării fiecărui incident.

Menționăm că exemplele de mai jos sunt pur fictive și sunt introduse strict în scop edificator.

Exemplul 1

Incident produs la data de 26.01.2014, la ora 11:40 descoperit la data de 26.01.2014 la ora 11:41.

Servicii și număr de conexiuni afectate per serviciu: 6.050 de conexiuni afectate/Servicii de telefonie furnizate prin intermediul unor rețele publice mobile terestre și 5.980 de conexiuni afectate/ Servicii de acces la Internet Conexiuni radio mobile (inclusiv MVNO)

Număr total de conexiuni afectate de incident: 12.030 de conexiuni afectate

Resursele afectate: – Stații de bază și controlere mobile - 2 BTS 3G/rețeaua de acces/nivel suport

Durata incidentului: 165 minute

Județe afectate: 1 județ afectat, Gorj – Târgu Jiu

Impact asupra apelurilor de urgență: Da (Apelurile nu s-au putut realiza prin rețeaua proprie)

Descrierea incidentului (detaliere a succesiunii evenimentelor, pentru a putea avea o imagine a ceea ce s-a întâmplat):

Datorită unei avarii la furnizorul de energie electrică 2 stații de bază au trecut pe alimentarea de back-up pe baterii. După 2 ore, stațiile de bază au devenit nefuncționale în urma descărcării bateriilor. Utilizatorii nu au putut utiliza serviciile mobile de voce si internet.

Cauza incidentului: Fenomen natural corelat cu Cauză externă/parte terță

Mai multe informații despre cauză: Datorită ninsorilor abundente s-a defectat un echipament al furnizorului de energie electrică ce a condus la intrarea funcționării a 2 site-uri 3G pe baterii.

Acțiuni de răspuns la incident (inclusiv momentul când au fost luate)

11:40 Întreruperea alimentării cu energie electrică datorită fenomenelor meteorologice ce au afectat un echipament al furnizorului de energie electrică/intrarea în funcțiune a bateriilor;

11:41 Detectarea incidentului;

11:55 Identificarea serviciilor impactate;

13:30 Deplasarea echipei de intervenție a fost întârziată din motive meteorologice nefavorabile;

13:41 Descărcarea bateriilor şi nefuncționarea celor 2 site-uri 3G;

14:25 S-a transportat și instalat la site un grup electrogen;

14:50 Serviciile nu mai sunt impactate.

Măsurile luate sau planificate pentru a împiedica producerea unui incident similar:

Upgrade autonomie baterii de la 2 ore la 4 ore.

Exemplul 2

Incident produs la data de 05/05/2013 la ora 16:34 descoperit la data de 05/05/2013 la ora 16:35.

Servicii și număr de conexiuni afectate per serviciu: 150.000 de conexiuni afectate/'Servicii de transmisiuni de date Mobil

Număr total de conexiuni afectate de incident: 150.000 de conexiuni afectate

Resurse afectate – Centre de mesagerie mobilă-3 noduri de trafic P2P MMS/nivel logic/rețeaua de acces

Durata incidentului: 75 minute

Județe afectate: 8 județe afectate – Bihor, Sălaj, Cluj, Alba, Arad, Timiș, Hunedoara, Mureș

Impact asupra apelurilor de urgență: Nu

Descrierea incidentului (detaliere a succesiunii evenimentelor, pentru a putea avea o imagine a ceea ce s-a întâmplat):

Din cauza creșterii numărului de conexiuni dintre nodurile de trafic de MMS și cele 2 servere care conțin baza de date cu utilizatorii, aceștia nu au putut utiliza serviciile de MMS.

Cauza incidentului: Eroare de sistem

Mai multe informații despre cauză:

În perioada sărbătorilor s-a înregistrat un trafic de MMS cu 40% mai crescut decât media normală, numărul de interogări în bazele de date a crescut ducând la un blocaj temporar de accesare a bazei de date.

Acțiuni de răspuns la incident (inclusiv momentul când au fost luate):

16:35 Detectarea incidentului prin intermediul alarmelor de monitorizare de către departamentul de Front Office;

16:40: Evaluarea impactului asupra serviciului;

16:45: Comunicarea problemei si a impactului de către departamentul de Front Office către client prin folosirea unei aplicații care trimite automat SMS-uri către clienți;

17:00 Restartarea de către departamentul de Back Office a procesului responsabil de comunicarea cu serverele de trafic de MMS de pe serverele care conțin bazele de date;

17:10 Restartarea procesului care stă la baza aplicației MMS pe toate nodurile de trafic de MMS;

17:12 Verificarea alarmelor și a erorilor din logurile de aplicație care arătau că problema nu s-a rezolvat;

17:35 Verificarea alarmelor și a erorilor din logurile de aplicație care arătau că problema s-a rezolvat; verificarea faptului că numărul de MMS-uri trimise pe secundă a revenit la normal.

17: 50 Serviciile nu mai sunt impactate.

17:55 Anunțarea clienților despre restabilirea serviciului și analiza cauzei și a măsurilor care se vor lua pentru a se evita acest tip de incident pe viitor.

Măsurile luate sau planificate pentru a împiedica producerea unui incident similar:

Upgrade de software/patch de soft planificat în data de 14.05.2014 ora 01:00 pentru ca impactul asupra traficului să fie cât mai scăzut.

6. RAPORTAREA UNUI INCIDENT FOLOSIND APLICAŢIA ONLINE

Conform Deciziei președintelui ANCOM nr. 512/2013, transmiterea notificării finale şi după caz a celei suplimentare se realizează exclusiv prin intermediul unei aplicații disponibile pe pagina de internet a ANCOM, ca înscris în formă electronică, căruia i s-a încorporat, atașat sau i s-a asociat logic o semnătură electronică extinsă, bazată pe un certificat calificat nesuspendat sau nerevocat la momentul respectiv şi generată cu ajutorul unui dispozitiv securizat de creare a semnăturii electronice, prevederile Deciziei președintelui Autorității Naționale pentru Administrare şi Reglementare în Comunicații nr. 336/2013 privind mijloacele şi modalitatea de transmitere a unor documente, date sau informații către Autoritatea Națională pentru Administrare şi Reglementare în Comunicații şi privind modificarea Deciziei președintelui Autorității Naționale pentru Comunicații nr. 77/2009 privind obligațiile de informare a utilizatorilor finali de către furnizorii de servicii de comunicații electronice destinate publicului fiind aplicabile în mod corespunzător.

Astfel, formularul de raportare a incidentelor cu impact semnificativ aferent notificării finale trebuie completat de către furnizorul de rețele şi servicii de comunicații electronice prin intermediul aplicației online SSCPDS - Sistemul Software de Colectare şi Prelucrare a Datelor Statistice (https://statistica.ancom.org.ro:8000/sscpds/index.faces). Aplicația este accesibilă din pagina principală a site-ului ANCOM (http://www.ancom.org.ro), apăsând butonul *Raportează.*

Pentru autentificare, se folosesc datele (numele de utilizator şi parola) utilizate de reprezentantul furnizorului pentru completarea datelor statistice ce trebuie raportate ANCOM.

Pentru informații privind accesul în aplicație, autentificarea şi gestionarea profilului utilizatorului, funcția de administrare a persoanelor autorizate, completarea datelor, semnarea electronică a formularelor, se recomandă consultarea manualului pentru utilizator FRSCE disponibil în format electronic pe pagina principală a aplicației.

Fig. 2 Prima pagina din aplicație după autentificare şi alegerea Completării unui formular

Pentru completarea/modificarea formularului de raportare a incidentelor cu impact semnificativ, din pagina principală a aplicației se accesează tab-ul *Gestionare Formulare -> Completare Formulare* (fig.2), iar din lista anchetelor aflate în desfășurare, conform figurii 3, se alege ancheta cu mnemonica *A151617008_D512_A2* şi titlul *D512 Anexa 2: Incidente cu impact semnificativ (permanent)*.

Mnemonică Anchetă	Descriere Anchetă	Stare Validare Date	Execută Validare	Completare
A002013005_D987_AINT	Acorduri interconectare (permanent)	Valid		
A002013005_D987_AACC	Acorduri acces la bucla locala (permanent)	Valid		
T021313005_D15_A1	Indicatori statistici privind furnizarea serviciilor de linii inchiriate T2 2013	Nevalidat		
A002013022_D987_A	Contracte privind dreptul de acces pe proprietăți (permanent)	Valid		
A002013005_CER_INTER	Cereri interconectare (permanent)	Valid		
A151617008_D512_A2	D512 Anexa 2: Incidente cu impact semnificativ (permanent)	Nevalidat		
A001314002_D333	D333 venituri si investitii anul 2013 (termen 31.05.2014)	Nevalidat		
A001314038_TARIF_MON	Tarif de monitorizare 2013 (termen iunie 2014)	Nevalidat		

Fig. 3 Alegerea anchetei cu mnemonica A151617008_D512_A2 şi titlul D512 Anexa 2: Incidente cu impact semnificativ (permanent).

Formularul se poate completa fie în modul online, fie în modul offline așa cum se poate observa din figura 4.

Fig. 4 Posibilități de completare a Formularului de raportare a incidentelor cu impact semnificativ

Pentru varianta completării offline, este disponibilă numai descărcarea în format XLSX a formularului de raportare (varianta PDF nu poate fi generată automat de sistem din cauza dimensiunii formularului/numărului mare de coloane). Este necesară alegerea numărului de rânduri dinamice ce pot fi completate adițional, adică numărul incidentelor ce urmează a fi raportate ANCOM la acel moment. Fișierul XLSX va fi încărcat în aplicație după completarea şi semnarea electronică a acestuia.

Înainte de completare se recomandă citirea instrucțiunilor anchetei şi a instrucțiunilor formularului (fig. 5) disponibile deasupra formularului propriu-zis printr-un click pe ⊕.

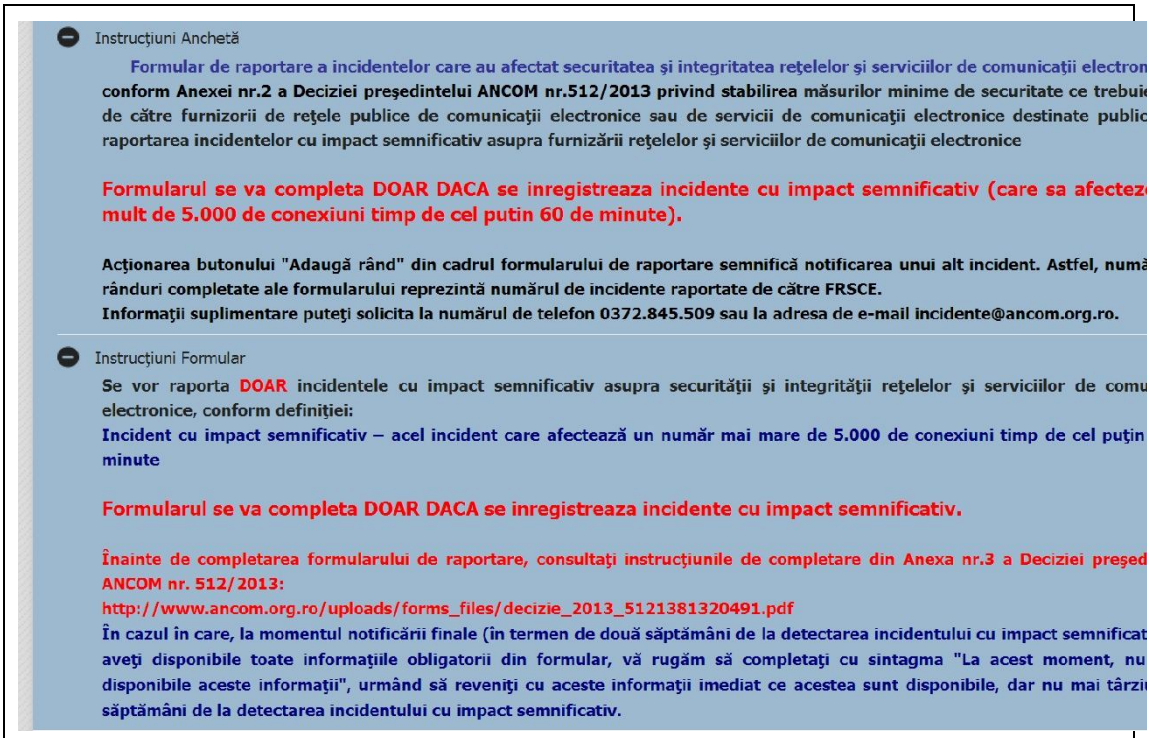

Fig. 5 Instrucțiuni Anchetă și instrucțiuni Formular din cadrul aplicației online

Pentru introducerea unui nou incident în aplicație, furnizorul va adăuga un nou rând la tabel.

Formularul este prezentat sub forma unui tabel cu 47 de coloane care reflectă informațiile solicitate în Anexa nr.2 a Deciziei președintelui ANCOM nr. 512/2013.

Se vor completa numele, adresa de poștă electronică și numărul de telefon al unei persoane de contact în cazul fiecărui incident raportat. Acest lucru este necesar pentru a se putea păstra contactul cu persoana responsabilă, pentru clarificări sau completări privind un anumit incident.

În cele ce urmează sunt redate o serie de îndrumări privind modul de completare a datelor solicitate în vederea validării unui incident cu impact semnificativ.

Astfel:

- completarea necorespunzătoare a unui câmp duce la atenționarea asupra tipului valorilor introduse (de exemplu, dacă la câmpul coloanei C30 ce desemnează numărul total de conexiuni afectate de incident vor fi introduse caractere alfanumerice, atenționarea va fi: *Acest câmp acceptă valori numerice*);

- câmpurile coloanelor C1-C5, C30-C45 au caracter obligatoriu, necompletarea sau completarea deficitară a acestora ducând la nevalidarea formularului;

- câmpul coloanelor C2 (data la care s-a produs incidentul), respectiv C4 (data la care s-a descoperit incidentul) vor fi completate cu date valide având formatul zz.ll.aaaa. Aceste date pot fi introduse fie de la tastatură, fie prin selectare din calendar;

- câmpul coloanelor C3, respectiv C5 (orele la care s-a produs, respectiv descoperit incidentul) vor fi completate cu ore/momente de timp valide având formatul hh:mm (00:00 - 23:59). Orele pot fi introduse fie de la tastatură, fie prin selectare din lista predefinită în cazul în care ora ce trebuie completată se regăsește în listă (granularitatea listei este din 15 în 15 minute).

- câmpul coloanelor C6-C30 (numărul de conexiuni afectate per serviciu/totalul), C35 (durata incidentului exprimată în minute), respectiv C36 (numărul judeţelor afectate) acceptă numai valori numerice;

- câmpul coloanei C31 va fi completat prin selectarea categoriei/categoriilor de resurse ce au fost afectate de incident (permite selecţie multiplă);

- câmpul coloanei C33 va fi completat prin alegerea categoriei de reţea (acces, centrală sau interconectare) care descrie localizarea resurselor/echipamentelor afectate în cadrul reţelei (permite selecţie unică);

- câmpul coloanei C34 va fi completat prin selecţia nivelului sau nivelurilor (fizic, logic sau suport) ce corespund afectării resurselor de către respectivul incident (permite selecţie multiplă);

- câmpul coloanei C39 (dacă incidentul a avut impact asupra apelurilor de urgență) va fi completat prin alegerea variantei corespunzătoare (permite selecție unică da/nu);

- câmpul coloanei C42 (cauza incidentului) va fi completat prin alegerea uneia sau mai multor opțiuni/tipuri ale cauzei incidentului în funcție de situație (permite selecție multiplă);

- câmpurile coloanelor C1, C32, C37, C38, C40, C41, C43-C47 acceptă orice tip de valori (şir de caractere);

- câmpurile tabelului ce necesită introducerea unor informații (indiferent de tipul valorilor introduse) permit introducerea unui număr foarte mare de caractere – maxim 100.000, fiind astfel posibilă descrierea corectă, completă/amănunțită a tuturor aspectelor solicitate pentru oferirea unei imagini cât mai clare asupra incidentelor petrecute;

- după introducerea informațiilor despre un incident, acestea vor fi salvate prin apăsarea butonului *Salvează*;

La nivel de formular, există mai multe reguli de validare a unui incident introdus, astfel:

- numărul total de conexiuni afectate de incident (valoarea introdusă la C30) trebuie să fie mai mare decât 5.000;

- numărul total de conexiuni afectate de incident (valoarea introdusă la C30) trebuie să fie egal cu suma conexiunilor afectate pe fiecare tip de serviciu (suma valorilor introduse în coloanele [C6-C29]);

- durata incidentului (valoarea introdusă la C35) trebuie să fie cel puțin egală cu 60 de minute.

Dacă regulile enumerate mai sus nu sunt respectate, după salvarea modificărilor, va apărea un mesaj de atenționare asupra încălcării unor corelații, respectiv un mesaj de eroare prin care va fi posibilă vizualizarea erorilor întâmpinate la completarea formularului.

Astfel de mesaje sunt exemplificate în figurile 6 şi 7:

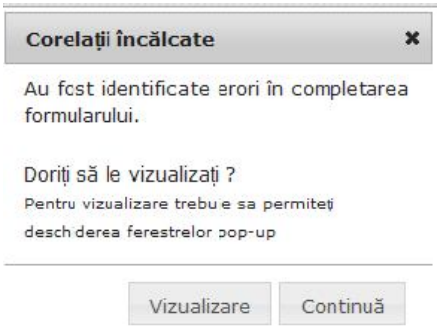

Fig. 6 Corelații încălcate

Fig. 7 Erori întâmpinate la Completarea Formularului

Corectarea tuturor erorilor va conduce la apariția mesajului *Datele chestionarului au fost validate cu succes*.

Pentru semnarea electronică, furnizorul trebuie să descarce formularul în format XLSX (varianta PDF nu poate fi generată automat de sistem din cauza dimensiunii formularului/numărului mare de coloane), să aplice semnătura electronică și apoi să încarce formularul semnat în aplicație. Se recomandă consultarea secțiunii dedicate din manualul pentru utilizator FRSCE disponibil în format electronic pe pagina principală a aplicației unde sunt descriși toți pașii ce trebuie parcurși în acest sens.

ANEXA 1 GLOSAR DE TERMENI PENTRU RESURSELE CE POT FI AFECTATE

- ***Stații de bază și controlere mobile***

  BTS (Base Transceiver Station) este o stație de bază de emisie-recepție din rețeaua de telefonie mobilă situată în partea de acces, care asigură comunicarea wireless între echipamentele de utilizator (UE) și rețea.

  BSC (Base Station Controller) este controlerul stației de bază și realizează, în partea de acces a rețelelor mobile, controlul BTS-urilor. De obicei, un BSC are zeci sau chiar sute de BTS-uri aflate sub controlul său.

  NodeB/eNodeB. NodeB este stația de bază de emisie-recepție în rețele de telefonie mobilă UMTS echivalentă cu BTS utilizată în GSM; Evolved NodeB (eNodeB) este stația de bază de emisie-recepție în rețele de telefonie mobilă LTE.

  RNC (Radio Network Controller) este controlerul de rețea radio din rețeaua de acces mobil UMTS (UTRAN) și este responsabil pentru controlul NodeB-urilor care sunt conectate la acesta. RNC realizează managementul resurselor radio, unele dintre funcțiile de gestionare a mobilității și este punctul în care se face criptarea datelor înainte de a fi trimise la și de la telefonul mobil al utilizatorului.

  MME (Mobility Management Entity) este nodul de control cheie pentru rețeaua de acces LTE. Acesta este responsabil pentru procedura de urmărire și paging, inclusiv retransmisia în modul de așteptare (idle) al UE (echipament de utilizator).

  ANDSF (Access Network Discovery and Selection Function) este situat în rețeaua centrală LTE și ajută echipamentul utilizatorului (UE) să descopere rețele de acces non-3GPP, cum ar fi Wi-Fi sau WiMAX - care pot fi utilizate pentru comunicații de date în plus față de rețele de acces 3GPP (cum ar fi HSPA sau LTE) și pentru a oferi UE regulile de conectare la aceste rețele.

  PCRF (Policy and Charging Rules Function) realizează stabilirea normelor de politică într-o rețea multimedia. PCRF joacă un rol central în rețelele IP de ultimă generație.

- ***Centre de comutație în rețele mobile***

  MSC (Mobile Switching Centre) este centrul de comutare a unei rețele de telefonie mobilă și are interfețe către BSC-uri, HLR, VLR și alte MSC-uri. MSC asigură comutarea apelurilor, managementul mobilității și servicii mobile pentru UE aflate în roaming în interiorul zonei pe care o deservește (voce, servicii fax, date, SMS, transferare a apelurilor).

  SGSN (Serving GPRS Support Node) realizează transportul pachetelor de date de la și către stațiile de bază din aria sa geografică de acoperire.

  GGSN (Gateway GPRS Support Node) realizează legătura între rețeaua GPRS (General Packet Radio Service) și rețelele externe cu comutație de pachete.

  PGW/PDN GW (Public Data Network Gateway): GW-ul PDN oferă conectivitate UE la rețelele externe de pachete de date, fiind punctul de intrare și ieșire al traficului pentru UE. PGW aplică politica de securitate și realizează filtrarea de pachete pentru fiecare utilizator, suport pentru taxare, interceptarea legală și screening-ul de pachete. Un alt rol cheie al PGW este de a acționa ca ancoră pentru mobilitatea între tehnologiile 3GPP și non-3GPP.

SGW (Serving Gateway) rutează și redirecționează pachetele de date de utilizator, în timp ce se comportă ca ancora de mobilitate pentru planul de utilizator în timpul handover-ului între eNodeB-uri și ca ancoră pentru mobilitatea între LTE și alte tehnologii 3GPP.

ePDG (Evolved Packet Data Gateway) securizează transmisia datelor dintre UE-uri conectate la EPC (Evolved Packet Core) peste rețele non 3GPP nesecurizate.

- ***Registrii de localizare***

  HLR (Home Location Register) este baza de date centrală într-o rețea mobilă care conține informații despre fiecare abonat care este autorizat să acceseze/să se conecteze la rețeaua centrală GSM.

  VLR (Visitor Location Register) este baza de date a abonaților rețelei mobile din aria de acoperire a MSC-ului. Fiecare stație de bază din rețea este deservită de câte un VLR.

  HSS (Home Subscriber Server) este baza de date ce conține profilurile abonaților și serviciile la care aceștia au acces. HSS realizează funcția de autentificare și autorizare a abonaților și poate furniza informații privind localizarea și IP-ul acestora.

  AuC (Authentication Centre) este o componentă a rețelei ce realizează funcția de autentificare/validare a informațiilor de securitate a cartelelor SIM ce încearcă să se conecteze la rețea.

- ***Centre de mesagerie mobilă***

  SMSC (Short Message Service Centre) este centrul serviciului de mesagerie scurtă ce stochează, redirecționează, modifică și transmite mesaje SMS.

  MMSC (Multimedia Messaging Service Centre) este centrul serviciului de mesagerie multimedia ce stochează, redirecționează, modifică și transmite mesaje MMS.

- ***Routere şi switch-uri IP***

  DSLAM (Digital Subscriber Line Access Multiplexer) este un echipament din rețeaua de acces care conectează mai multe interfețe de linii digitale de abonat (DSL) la un canal de comunicații digitale de mare viteză folosind tehnici de multiplexare.

  BRAS rutează traficul către și dinspre dispozitive de acces broadband precum DSLAM în rețeaua unui ISP.

  Metro router este un sistem de rutare a traficului în rețele de acoperire metropolitană.

  Metro switch este un dispozitiv care realizează interconectarea diferitelor segmente din rețele de acoperire metropolitană.

  EDGE routers sunt routere situate la marginea rețelei IP a furnizorului.

  IP PBX (Private Branch Exchange) este un sistem de rutare și comutare a apelurilor telefonice într-o rețea de telefonie IP.

  Core routers sunt routere situate în rețeaua centrală (core) a furnizorului.

- ***Echipamente din noduri de transmisiune***

  SDH (Synchronous Digital Hierarchy) sunt protocoale standardizate care transferă în mod sincron mai multe fluxuri digitale de biți pe fibră optică.

PDH (Plesiochronous Digital Hierarchy) este o tehnologie folosită în rețelele de telecomunicații pentru a transporta cantități mari de date prin rețele digitale de mari dimensiuni.

DWDM (Dense/Wavelength-Division Multiplexing) este o tehnologie prin care se multiplexează un număr de semnale purtătoare optice pe o singură fibră optică utilizând lungimi de undă diferite (de exemplu culori) de lumină laser. Această tehnică permite comunicații bidirecționale peste un fir de fibre.

- ***Puncte de interconectare***

  IXP (Internet eXchange Point) este o infrastructură fizică prin care furnizorii de servicii de acces la Internet (ISP) realizează transfer de trafic IP între rețelele lor.

  POI (Point Of Interconnection) este un punct în rețeaua furnizorului de comunicații electronice de interconectare cu alte rețele.

- ***Servere de adresare***

  DHCP (Dynamic Host Configuration Protocol) este un protocol și un serviciu care alocă o adresă IP sistemelor din rețea.

  DNS (Domain Name System) este un sistem distribuit de denumire a computerelor, serviciilor sau oricăror alte resurse conectate la Internet sau rețea privată. Acesta asociază diferite informații cu nume de domenii alocate fiecărei entități participante.

- ***Sisteme de securitate***

  IDS (Intrusion Detection System) este sistemul de detectare a intruziunilor care este utilizat pentru identificarea unor încercări de intruziuni, intruziuni ce au sau au avut loc și eventual pentru răspunsul la intruziuni în rețele și sisteme informatice.

  IPS (Intrusion Prevention System) este sistemul de prevenire a intruziunilor care este utilizat pentru identificarea și prevenirea unor încercări de intruziuni sau intruziuni ce au loc în rețele și sisteme informatice.

  AAA (authentication, authorization and accounting or auditability) se referă la o arhitectură de securitate a sistemelor distribuite în cadrul căreia se autentifică identitatea utilizatorului, se acordă acces acestuia și în final se menține o înregistrare a accesului acestuia pentru taxare și auditare.

  LDAP (Lightweight Directory Access Protocol) este un protocol de accesare și administrare a directorului cu informații privind utilizatorii și drepturile de acces ale acestora. De obicei, LDAP este utilizat pentru a găsi rapid informații despre un anumit utilizator în directoare cu foarte mulți utilizatori.

  VPN (Virtual Private Network) conectează componentele și resursele unei rețele private prin intermediul unei rețele publice.

  FIREWALL este un sistem de securitate al rețelei, de tip software sau hardware, care controlează traficul ce iese și intră în rețea analizând pachetele de date și determinând pe baza unui set de reguli de securitate dacă acestea pot pătrunde în rețea sau nu.

- ***Componente/Platforme de servicii***

  IPTV (Internet Protocol TeleVision) este o platformă de servicii prin care se transmit programe audio-vizuale într-o rețea care se bazează pe IP.

  VoIP (Voice over IP) este o platformă prin care se oferă servicii de transmitere a semnalelor vocale prin rețele IP.

  IMS (IP Multimedia Subsystem) este o platformă în rețelele de generație viitoare prin care se pot oferi servicii multimedia fixe sau mobile.

  STP (Signal Transfer Point) este o componentă a rețelelor inteligente (de telefonie fixă și mobilă) care comută mesajele SS7 între SEP-uri (Signalling End-Point) și alte STP-uri.

  SCP (Service Control Point) este o componentă standard a rețelelor inteligente (de telefonie fixă și mobilă) utilizată pentru administrarea serviciilor oferite în aceste rețele.

- ***OSS*** (Operations Support Systems) și **BSS** (Business Support Systems) sunt platforme informatice utilizate de furnizorii de servicii de comunicații electronice în scopul administrării propriilor rețele. Aceste platforme realizează funcții precum managementul, inventarierea și configurarea rețelei. De asemenea, se mai ocupă cu managementul rețelei în cazul incidentelor.