ANCOM
Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii

RAPORT
privind implementarea măsurilor de securitate în domeniul managementului incidentelor

aprilie 2017

Cuprins

Introducere 2
I. Procese și proceduri privind managementul incidentelor 4
1. Politica de management al incidentelor 4
2. Echipa de răspuns la incidente 5
3. Schema de management al incidentelor 6
3.1 procese corespunzătoare schemei de management al incidentelor 7
3.1.1 detectare și raportare 7
3.1.2 evaluare/triere și decizie 8
3.1.3 răspuns 9
3.1.4 escaladare 10
3.1.5 colectarea informațiilor despre incidente și păstrarea evidenței acestora 11
3.1.6 automatizarea 12
3.1.7 incidente cibernetice 13
3.2 proceduri corespunzătoare schemei de management al incidentelor 14
4. Evaluarea schemei de management al incidentelor și îmbunătățiri 15
4.1 analiza incidentelor și organizarea unor întâlniri 15
4.2 evaluarea schemei de management al incidentelor 16
4.3 îmbunătățiri ale măsurilor de securitate 16
II. Sistem de detectare a incidentelor 17
1. Sistem de detectare a incidentelor 17
1.1 primirea sesizărilor și notificărilor despre incidente din partea unor persoane 18
1.2 sisteme de monitorizare automată 18
1.2.1 monitorizarea rețelelor și serviciilor de comunicații electronice 18
1.2.2 monitorizarea rețelei interne 20
1.2.3 monitorizarea accesului în locații 22
1.2.4 monitorizarea mediului 23
1.3. Detectare proactivă 23
2. Evaluarea și actualizarea sistemului de detectare 23
III. Proceduri și planuri de comunicare a incidentelor 24
1. Proceduri de raportare a incidentelor către ancom, precum și către alte autorități responsabile 25
2. Planuri de comunicare către alte părți 25
3. Evaluarea și actualizarea planurilor și procedurilor de comunicare sau raportare a incidentelor 26
IV. Alte informații 27
V. Concluzii 31
VI. Anexă - lista furnizorilor către care s-a transmis chestionarul 34

Introducere

În vederea asigurării unor comunicații fiabile și sigure prin intermediul rețelelor publice de comunicații electronice, potrivit dispozițiilor art. 46 din 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, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului trebuie să adopte și să implementeze toate măsurile adecvate, de ordin tehnic și organizatoric, în vederea administrării riscurilor la adresa securității și integrității rețelelor și serviciilor de comunicații electronice.

În acest sens, art. 3 din Decizia președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații 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 și raportarea incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice[1] prevede următoarele:

„Art. 3. – (1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a lua toate măsurile de securitate adecvate pentru a administra riscurile la adresa securității rețelelor și serviciilor de comunicații electronice, astfel încât să asigure un nivel de securitate corespunzător riscului identificat și să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor și rețelelor interconectate, având în vedere cele mai noi tehnologii și, acolo unde este cazul, de a colabora cu alți furnizori pentru implementarea acestor măsuri.

(2) Furnizorii de rețele publice de comunicații electronice au obligația de a lua toate măsurile de securitate necesare pentru a administra riscurile la adresa integrității rețelelor și serviciilor de comunicații electronice, în scopul garantării integrității rețelelor și al asigurării continuității furnizării serviciilor prin intermediul acestor rețele și, acolo unde este cazul, de a colabora cu alți furnizori pentru implementarea acestor măsuri.

(3) Măsurile minime de securitate pe care trebuie să le stabilească și să le implementeze furnizorii, astfel încât să îndeplinească obligația prevăzută la alin. (1) și, după caz, cea prevăzută la alin. (2) vor viza cel puțin domeniile identificate în anexa nr. 1.

(4) Furnizorii au obligația de a evalua și, dacă este cazul, de a actualiza măsurile prevăzute la alin. (3) ori de câte ori este necesar, însă cel puțin o dată la 12 luni."

În 2016, ANCOM a realizat și publicat Ghidul[2] de implementare a măsurilor de securitate în domeniul managementului incidentelor conform Deciziei nr.512/2013, cu scopul de a oferi îndrumări furnizorilor de rețele și servicii de comunicații electronice în vederea implementării unor măsuri care să respecte prevederile legale ale deciziei menționate mai sus, contribuind la îmbunătățirea securității și integrității rețelelor și serviciilor de comunicații electronice, din perspectiva managementului incidentelor. Ghidul oferă îndrumări și recomandări privind implementarea anumitor măsuri, însă alegerea măsurilor specifice aparține furnizorilor de rețele și servicii de comunicații electronice, care vor ține cont în alegerea lor de factori precum rezultatele evaluării riscurilor în cadrul organizației, ale estimării impactului incidentelor asupra furnizării serviciilor de comunicații electronice, profilul organizației (tipurile de rețele și servicii oferite, numărul utilizatorilor de servicii, numărul conexiunilor de acces etc.).

În vederea monitorizării implementării prevederilor Deciziei nr.512/2013, ANCOM a elaborat *Raportul privind implementarea măsurilor de securitate în domeniul managementului incidentelor*, având drept scop evaluarea securității și integrității rețelelor și serviciilor de comunicații electronice din perspectiva măsurilor de securitate implementate de furnizori în acest domeniu, conform prevederilor legale.

---

[1] Decizia preşedintelui Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii nr. 512/2013 privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului şi raportarea incidentelor cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice se găseşte la adresa: http://www.ancom.org.ro/formdata-1130-48-1703

2 Ghidul poate fi consultat la următoarea adresă:
http://www.ancom.org.ro/uploads/links_files/Ghid_de_implementare_a_masurilor_de_securitate.pdf

Pentru a evalua stadiul de implementare a măsurilor de securitate în domeniul managementului incidentelor, ANCOM a transmis către 31 de furnizori[3] de rețele și servicii de comunicații electronice un chestionar privind implementarea măsurilor de securitate în domeniul managementului incidentelor[4]. Furnizorii chestionați au fost cei care, pentru ultima perioadă de raportare stabilită conform prevederilor Deciziei președintelui ANCOM 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, au raportat un număr cuprins între 5.000 și 100.000 de conexiuni pentru serviciile de comunicații electronice. Cei 31 de furnizori de rețele și servicii de comunicații electronice chestionați au raportat aproximativ 360.000 de conexiuni în total.

Managementul incidentelor implică dezvoltarea unei politici de management al incidentelor, a unui set de procese și proceduri consistente, repetabile, măsurabile și utilizarea unor mijloace adecvate de natură administrativă, managerială, tehnică sau juridică în vederea detectării, analizei și răspunsului la incidentele ce au loc în cadrul organizației și care afectează/pot afecta procesele și obiectivele afacerii și implicit furnizarea rețelelor și serviciilor de comunicații electronice. Aplicarea unor procese și proceduri corespunzătoare pentru protecția rețelelor și serviciilor de comunicații electronice, acoperind resurse hardware, software (echipamente de rețea, sisteme, aplicații etc.) și alte tipuri de resurse ce pot fi implicate în procesul furnizării rețelelor și serviciilor de comunicații electronice este menită să conducă la reducerea frecvenței de apariție a incidentelor în cadrul organizației. Prevenirea incidentelor este de regulă mult mai eficientă și mai puțin costisitoare decât răspunsul, reacția la acestea. Astfel, este de regulă util ca organizația să-și orienteze activitățile de tratare a incidentelor nu numai spre acțiuni reactive, ci și spre eforturi proactive.

Având în vedere potențialul impact al incidentelor asupra propriei organizații și asupra utilizatorilor finali, managementul incidentelor reprezintă un element important, fundamental pentru asigurarea securității rețelelor și serviciilor, fiind necesar să i se acorde importanța cuvenită.

În cadrul chestionarului transmis, se aplică definițiile menționate în Decizia președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații nr.512/2013.

În urma centralizării și analizei răspunsurilor la chestionar, au fost identificate aspectele prezentate în cele ce urmează.

[3] Lista furnizorilor către care s-a transmis chestionarul se regăsește în anexa la prezentul raport.
[4] Chestionarul transmis furnizorilor este disponibil în format electronic pe pagina de internet a ANCOM la adresa: www.ancom.org.ro/uploads/links_files/Chestionar_masuri_de_securitate_in_domeniul_managementului_incidentelor.doc
Adresa de înaintare se găsește la adresa:
http://www.ancom.org.ro/uploads/links_files/Adresa_masuri_de_securitate_in_domeniul_managementului_incidentelor.pdf

I. Procese și proceduri privind managementul incidentelor

Conform Deciziei nr.512/2013, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația să stabilească procese și proceduri pentru managementul incidentelor care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice (care să vizeze raportarea internă, evaluarea, răspunsul la incidente și escaladarea acestuia), inclusiv prin definirea rolurilor și responsabilităților.

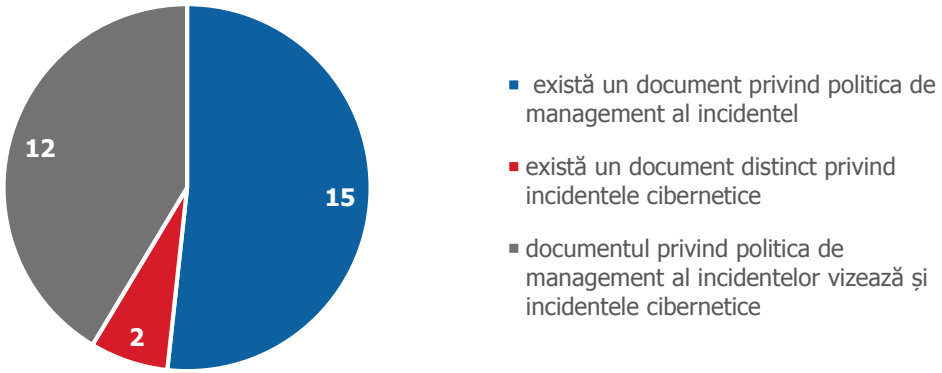
1. Politica de management al incidentelor

Politica de management al incidentelor reprezintă acel document care trasează o direcție clară a organizației în domeniul managementului incidentelor și la baza căruia stau procesele și procedurile aferente acestui domeniu, precum și resursele, mecanismele, capabilitățile (tehnice, operaționale etc.) ce susțin aceste procese și proceduri.

Conform răspunsurilor primite, 15 furnizori dețin o politică a managementului incidentelor, dintre care pentru 7 furnizori există un document distinct privind politica de management al incidentelor, separat de alte documente și pentru alți 8 furnizori, documentul privind politica de management al incidentelor este integrat în documentul politicii de securitate a organizației sau în alte documente interne.

Pentru 12 dintre furnizorii chestionați, această politică de management al incidentelor vizează și incidentele cibernetice[5]. 2 dintre furnizori au raportat că dețin o politică distinctă (un alt document de politică) privind aceste incidente. Figura 1 ilustrează situația furnizorilor chestionați în ceea ce privește existența unei politici de management al incidentelor.

Fig. 1 Politica de management al incidentelor



Conform răspunsurilor la chestionar, politica de management al incidentrelor conține:

Politica de management al incidentrelor conține	Nr. răspunsuri
Importanța procesului de management al incidentelor pentru organizație și angajamentul conducerii organizației în sprijinirea managementului incidentelor;	10
Scopul, obiectivele și domeniul de aplicare a politicii (cui se aplică, în ce condiții etc.);	10

[5] Conform Hotărârii Guvernului României nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, incidentul cibernetic este acel eveniment survenit în spaţiul cibernetic ale cărui consecinţe afectează starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private, din spaţiul cibernetic.

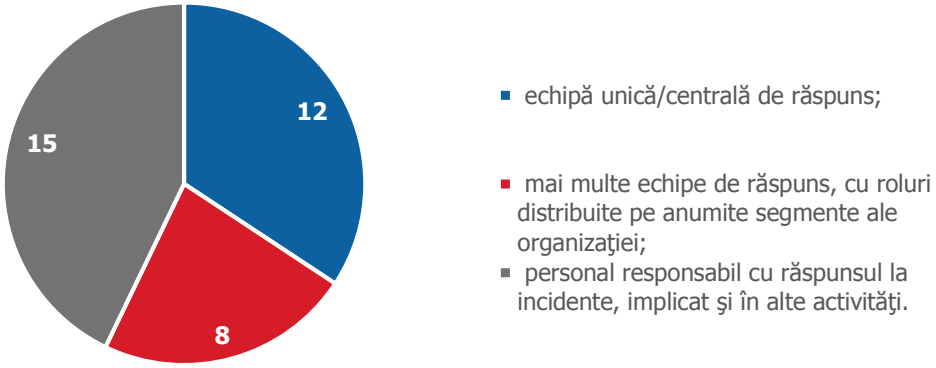
Definirea unor termeni specifici, încadrabili în contextul managementului incidentelor (de exemplu eveniment, incident, incident minor/major/critic, amenințare, vulnerabilitate, răspuns, escaladare, situație de urgență);	12
Modul de detectare, raportare și colectare a informațiilor despre evenimentele ce afectează sau care pot afecta securitatea, inclusiv prin corelarea acestor procese cu tipuri de incidente frecvente/predictibile;	14
Modul de analiză și evaluare (incluzând triere, prioritizare) a incidentelor;	11
Activitățile ce trebuie întreprinse în vederea inițierii răspunsului la incidentele confirmate;	12
Necesitatea înregistrării tuturor activităților desfășurate în vederea unor analize ulterioare și păstrarea sigură a evidenței privind incidentele înregistrate;	7
Activități post-incident incluzând evaluarea incidentelor și îmbunătățirea proceselor și procedurilor din cadrul schemei de management al incidentelor;	9
Activitățile de identificare, raportare și tratare a vulnerabilităților;	14
Documentația schemei de management al incidentelor (proceduri, formulare de raportare a incidentelor etc.);	6
Aspecte privind personalul care se ocupă de managementul incidentelor/echipa de răspuns la incidente:	14
Mecanismele, resursele, capabilitățile ce asigură suportul necesar (tehnic, operațional etc.);	14
Programul de conștientizare și instruire în domeniul managementului incidentelor;	6
Procesul de diseminare a informațiilor despre incidente unor părți externe;	4
Actele normative ce trebuie respectate și alte aspecte legale ce trebuie luate în considerare;	7

De regulă, politica, procesele și procedurile de management al incidentelor sunt disponibile întregului personal al organizației și se adresează cu precădere personalului cu atribuții de specialitate în domeniu (personalului tehnic implicat/entităților participante în procesele de detectare, rezolvare, închidere a incidentelor).

2. Echipa de răspuns la incidente

În ceea ce privește existența unei echipe de răspuns la incidente, toți furnizorii chestionați au afirmat că există personal/echipă de răspuns care se ocupă de tratarea/managementul incidentelor, având caracteristicile ilustrate în figura următoare:

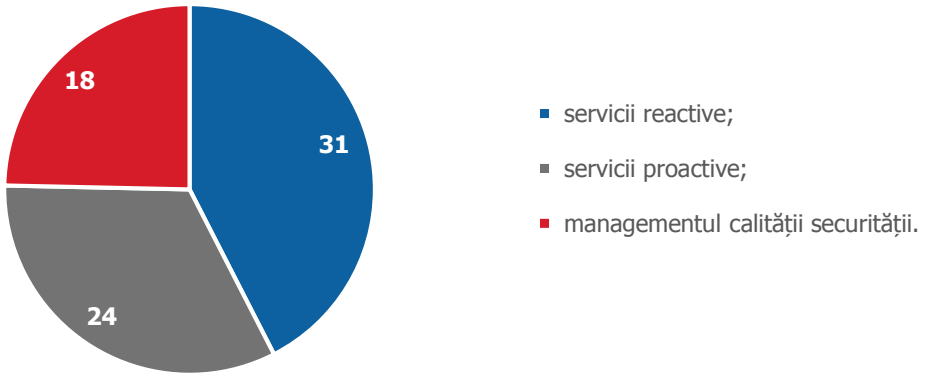
Fig. 2 Tipuri de echipe de răspuns raportate de furnizori (număr de răspunsuri per categorie)



Totodată, 19 furnizori au raportat că echipa de răspuns este disponibilă în timp real, 24/7.

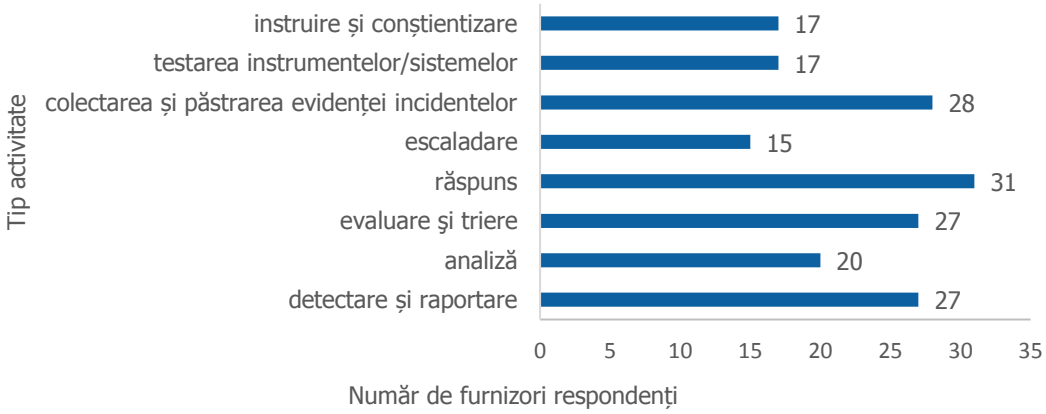
Managementul incidentelor este externalizat în totalitate în cazul a 2 furnizori și parțial în cazul a 11 furnizori.

Fig 3. Servicii acoperite de echipa de răspuns la incidente (număr de răspunsuri per categorie)



Conform răspunsurilor furnizorilor, echipa de răspuns desfășoară activități în ceea ce privește evenimentele/incidentele din organizație, precum:

Fig. 4 Tipuri de activități desfășurate de echipa de răspuns în ceea ce privește evenimentele/incidentele din organizație



În cazul a 21 de furnizori, tratarea incidentelor cibernetice este realizată în cadrul aceleiași echipe de răspuns la incidente și pentru 7 dintre furnizori, există o echipă dedicată privind tratarea incidentelor cibernetice. 3 furnizori nu tratează incidentele cibernetice.

3. Schema de management al incidentelor[6]

Stabilirea unei scheme de management al incidentelor este utilă pentru o gestionare/tratare cât mai eficientă a incidentelor. Această schemă trebuie să fie în concordanță cu politica de management al incidentelor. Pentru a fi eficiente, procesele și procedurile din cadrul schemei trebuie să definească fazele gestionării incidentelor, oferind îndrumări privind modul de detectare, analiză, clasificare și prioritizare, răspuns la evenimente/incidente/vulnerabilități, precum și indicații pentru identificarea îmbunătățirilor ce pot fi aduse întregului proces de management al incidentelor.

[6] **Schema de management al incidentelor** cuprinde procese şi proceduri documentate, detaliate, menite să asigure detectarea, analiza/evaluarea şi răspunsul eficient la evenimente/incidente/vulnerabilităţi ce afectează sau pot afecta procesele şi obiectivele afacerii, implicit securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice. **Procesele privind managementul incidentelor** vizează activităţile ce trebuie desfăşurate pentru soluţionarea incidentelor ce se petrec şi pentru prevenirea apariţiei/reapariţiei acestora. **Procedurile documentate privind managementul incidentelor** sunt acele proceduri întocmite pe baza proceselor de management al incidentelor, care vizează activităţile personalului implicat în detectarea, evaluarea, trierea, decizia şi răspunsul la incidente, inclusiv prin alocarea rolurilor şi responsabilităţilor corespunzătoare.

Răspunsurile la chestionar au indicat faptul că toți furnizorii chestionați dețin o schemă de management al incidentelor. În general, schema de management al incidentelor tratează etapele gestionării incidentelor, oferind îndrumări privind modul de detectare, analiză, clasificare, prioritizare, răspuns la evenimente, incidente, vulnerabilități.

3.1 Procese corespunzătoare schemei de management al incidentelor

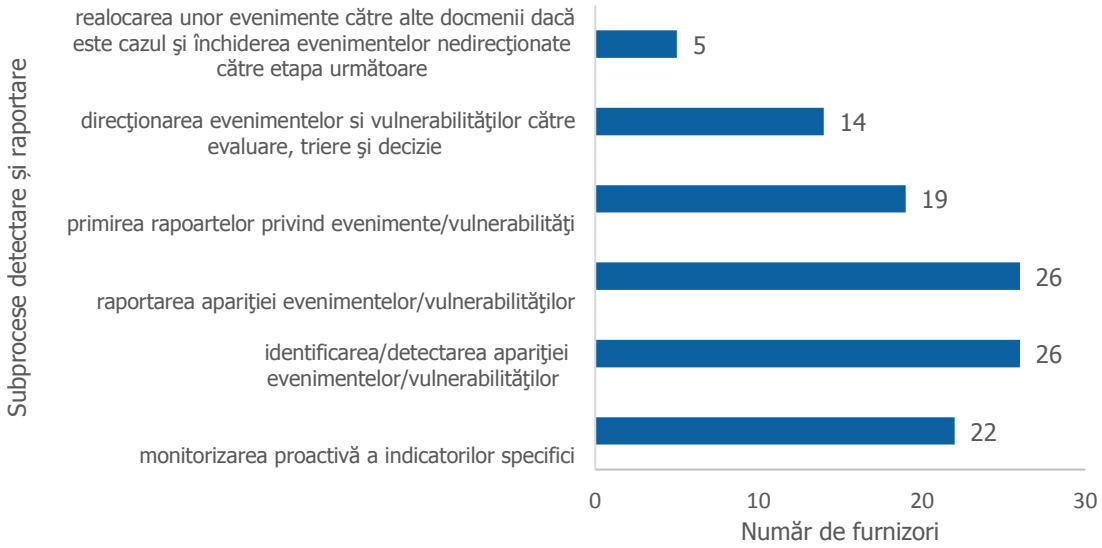
Sistemele utilizate pentru managementul incidentelor sunt independente de sisteme/echipamente implicate în furnizarea rețelelor și serviciilor de comunicații pentru 7 dintre furnizori și sunt testate periodic (inclusiv testarea periodică a echipamentelor de rezervă - back-up) de către 21 de furnizori.

3.1.1 Detectare și raportare

Toți furnizorii chestionați au raportat că există un proces de detectare și raportare internă a evenimentelor și incidentelor care afectează sau pot afecta securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

Procesul de detectare și raportare internă a evenimentelor/incidentelor cuprinde subprocese precum:

Fig. 5 Procesul de detectare



14 dintre furnizori au raportat că în cadrul procesului de detectare și raportare, vulnerabilitățile sunt luate în considerare.

Descrierea pe scurt a procesului de detectare și raportare a incidentelor a scos în evidență practici precum:

- detectarea incidentelor prin sisteme de monitorizare automată a disponibilității echipamentelor și a parametrilor de funcționare a echipamentelor, prin monitorizarea traficului și a logurilor, prin accesul direct pe echipamentele de rețea, pe baza informațiilor primite de la personalul intern, de la terți și din sesizările utilizatorilor finali;
- raportarea către compartimentele/echipele responsabile, fie în mod automat de către sistemele de monitorizare, fie manual prin intermediul apelului telefonic, SMS-ului sau email-ului;
- înregistrarea incidentelor în mod automat, prin intermediul aplicației de ticketing a organizației și manual, în centralizatoare ale incidentelor, pe suport electronic.

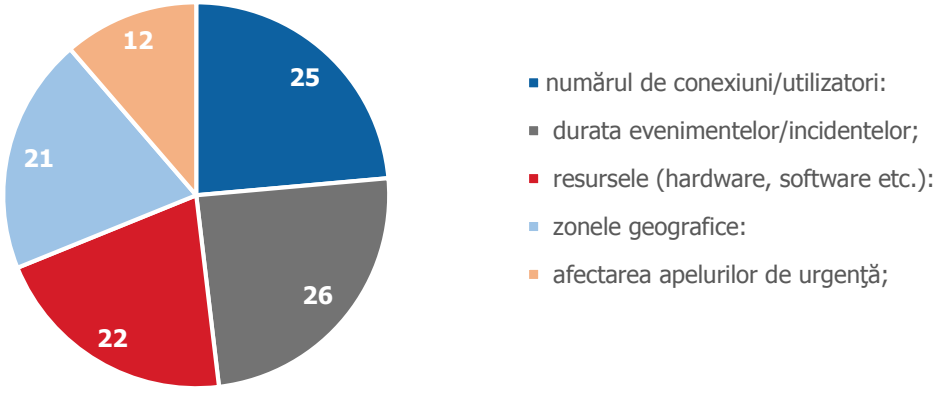
3.1.2 Evaluare/triere și decizie

Procesul de evaluare/triere și decizie se referă la acțiunile ce trebuie întreprinse după detectarea evenimentelor/vulnerabilităților în vederea determinării eventualelor incidente și asigurării unui răspuns rapid, eficient și organizat. Determinarea impactului incidentului asupra furnizării rețelelor și serviciilor de comunicații electronice, asupra proceselor afacerii pe baza încadrării acestuia în anumite categorii (de exemplu incidente minore, majore, critice) conduce, de regulă, la decizii asupra soluțiilor de remediere, modului de prioritizare a acțiunilor de răspuns, asupra nivelelor necesare de escaladare a răspunsului la incident.

Conform răspunsurilor primite, 27 de furnizori au afirmat că, în cadrul propriilor organizații, există un proces de evaluare/triere și decizie a evenimentelor/incidentelor care afectează/pot afecta securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

Procesul de evaluare/triere și decizie a evenimentelor/incidentelor cuprinde subprocese precum:	**Număr răspunsuri**
Analiză și evaluare inițială a evenimentelor/incidentelor/vulnerabilităților detectate;	23
Strângerea informațiilor despre incidente;	19
Diagnosticarea incidentelor (stabilirea cauzei);	23
Identificarea resurselor real sau potențial afectate, precum și localizarea acestora;	25
Determinarea/evaluarea impactului incidentelor folosind o clasificare/scală agreată (bazată pe definirea unor trepte de severitate) și clasificarea/încadrarea acestora în anumite categorii (de exemplu incidente – minore, majore, critice);	10
Corelarea cu alte evenimente/incidente/vulnerabilități trecute sau în curs de desfășurare;	17
Prioritizarea incidentelor în vederea răspunsului;	22
Analiza posibilităților de răspuns și decizii asupra modului de răspuns la incidente, precum și asupra nivelelor de escaladare;	11
Prioritizarea acțiunilor de răspuns;	17
Direcționarea incidentelor către etapa/procesul de răspuns, realocarea unor evenimente unor domenii externe procesului de management al incidentelor și închiderea evenimentelor nedirecționate către etapa următoare, dacă este cazul;	7
Evaluarea vulnerabilităților și luarea deciziilor privind tratarea lor.	12

Fig. 6 Determinarea impactului evenimentului/incidentului asupra furnizării reţelelor şi serviciilor de comunicaţii



26 dintre furnizori au raportat că realizează corelarea evenimentelor ad-hoc, 18 dintre aceștia afirmând că realizează corelarea și prin sisteme automate.

Totodată, 12 dintre furnziorii respondenți iau în considerare și vulnerabilitățile în cadrul procesului de evaluare, triere și decizie.

Descrierea pe scurt a procesului de evaluare, triere și decizie așa cum este implementat în cadrul organizației a evidențiat principalele activități ale furnizorilor chestionați în această privință:

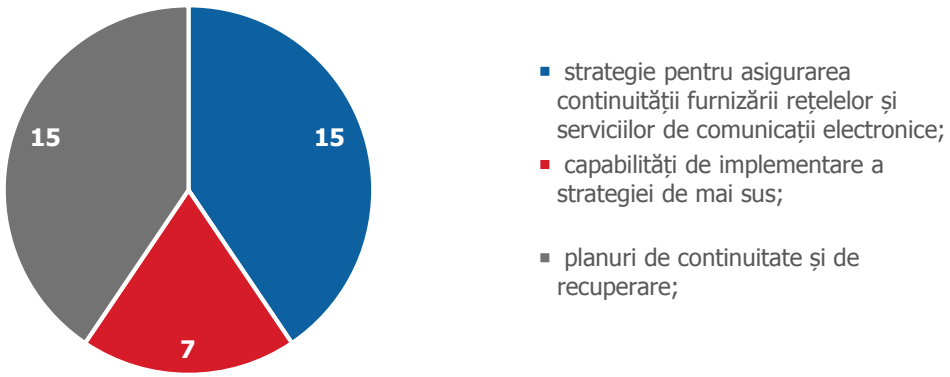
- analiza informațiilor despre incidente (alarme primite de la echipamente, notificări interne/externe primite etc.);
- evaluarea impactului incidentelor;
- evaluarea cauzei/cauzelor posibile a/ale incidentelor;
- clasificarea/trierea evenimentelor/incidentelor;
- identificarea serviciilor afectate;
- evaluarea resurselor ce sunt sau pot fi afectate de incidente;
- estimarea timpului de remediere;
- identificarea ariei de acoperire a incidentului.

3.1.3 Răspuns

Toți cei 31 de furnizori chestionați dețin un proces de răspuns la evenimente/incidente care afectează/pot afecta securitatea și integritatea rețelelor.

În cadrul procesului de răspuns la evenimente/incidente:	Număr respondenți
Sunt alocate roluri și responsabilități asociate răspunsului la incidente;	16
Se asigură răspunsul tehnic (asigurarea instrumentelor și a suportului tehnic) și managerial (coordonarea activităților de răspuns);	29
Există posibilitatea răspunsului imediat la incidente;	30
Există posibilitatea răspunsului ulterior/pe termen lung la incidente;	23
Se realizează activitățile necesare în caz de urgență/criză (eventual prin escaladarea la personalul corespunzător) sau în cazul unui impact major/sever asupra organizației/furnizării rețelelor și serviciilor de comunicații electronice;	21
Există un subproces de realocare a evenimentelor unor domenii externe procesului de management al incidentelor dacă este cazul și închiderea răspunsului/incidentului;	7
Există un subproces de corelare și monitorizare continuă a activităților de răspuns, concomitent cu verificarea statusului incidentului în vederea stabilirii dacă acesta este sau nu ținut sub control;	10
Există un subproces de monitorizare a rețelei/sistemelor/serviciilor după restabilirea funcționării acestora la parametri normali;	13

Fig. 7 Pentru situațiile generate de perturbări grave ale funcționării rețelei sau serviciului, organizația deține:



În descrierea subproceselor/activităților uzuale asociate răspunsului la evenimente/incidente, furnizorii au punctat acțiuni aferente întregului flux de management al incidentelor, de la detectare și raportare internă, până la remedierea/închiderea incidentelor.

Astfel, printre categoriile de acțiuni de răspuns imediat la incidente au fost menționate:

- organizarea activităților de răspuns/activități logistice (de exemplu organizarea echipelor de intervenție din punct de vedere al resurselor umane, al echipamentelor de intervenție, aspectelor referitoare la deplasare, dispecerizarea echipelor în teren pentru rezolvarea problemelor);
- utilizarea soluțiilor de backup/alternative (de exemplu folosirea unor circuite de rezervă/alternative, rerutarea serviciilor pe canale alternative, rerutarea traficului, alimentarea cu energie electrică cu ajutorul generatoarelor);
- izolarea echipamentelor/segmentelor/sistemelor afectate;
- remedierea problemelor prin aplicarea unor măsuri/soluții (de exemplu înlocuirea unor echipamente defecte, refacerea traseului de cablu deteriorat, depanarea sistemelor informatice, reconfigurarea/reinițializarea unor echipamente/sisteme software, reconfigurări de parametri, intervenția manuală, relocarea fizică, filtrarea IP-urilor, blocarea unor porturi);
- cooperarea cu alte părți - alți furnizori de rețele și servicii de comunicații electronice, furnizori de utilități, producători de echipamente etc. (de exemplu cooperarea cu furnizori de energie electrică, contactarea producătorilor de echipamente pentru escaladare).

Totodată, printre categoriile de acțiuni de răspuns ulterior/pe termen lung la incidente au fost menționate:

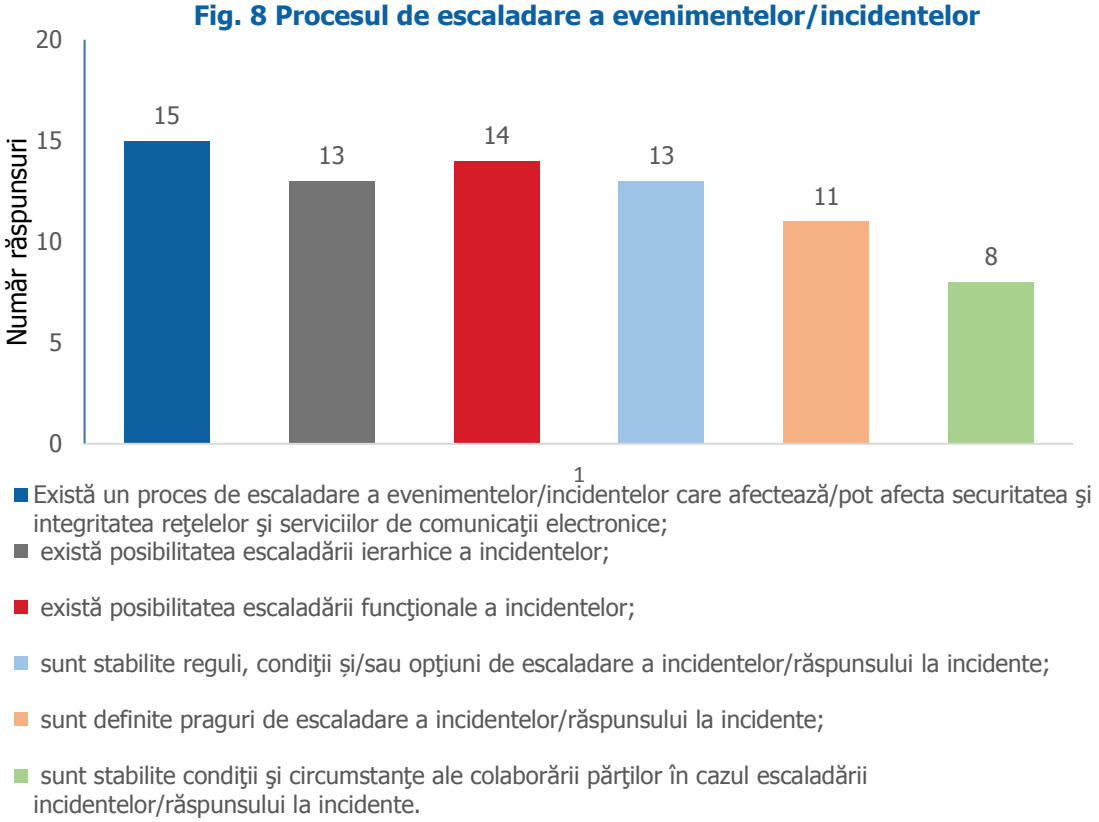
- acțiuni de remediere/restabilire completă a sistemelor/rețelelor/serviciilor;
- achiziționarea de echipamente pentru înlocuirea celor afectate;
- actualizarea proceselor, politicilor și procedurilor operaționale;
- implementarea unor soluții de back-up;
- schimbarea tehnologiilor/soluțiilor tehnice;
- modificări în configurația rețelei;
- creșterea capacității acumulatorilor;
- actualizarea instrumentelor software etc.

Conform răspunsurilor primite, 12 furnizori iau în considerare vulnerabilitățile în cadrul procesului de răspuns.

3.1.4 Escaladare

Figura 8 prezintă procesul escaladării incidentelor/răspunsului la incidente în rândul furnizorilor chestionați.

Fig. 8 Procesul de escaladare a evenimentelor/incidentelor



În rândul furnizorilor chestionați, necesitatea escaladării incidentelor/răspunsului la incidente depinde de:

- nivelul de impact al incidentului;
- intervalul de timp alocat remedierii incidentelor;
- schimbarea priorității de rezolvare a incidentului;
- cazurile în care resursele solicitate echipei de intervenție depășesc resursele alocate sau competențele atribuite. De regulă, furnizorii dețin nivele de escaladare în funcție de normele interne;
- aria de expertiză a diverselor părți implicate;
- depășirea unor praguri de timp prestabilite și asociate severității incidentului, în funcție de nivelul afectării *SLA*[7] etc.

3.1.5 Colectarea informațiilor despre incidente și păstrarea evidenței acestora

28 de furnizori au afirmat că există facilități/sisteme/instrumente tehnice și operaționale de colectare a informațiilor despre evenimente/incidente și țin o evidență a incidentelor petrecute în cadrul propriilor organizații. Dintre aceștia, 23 de furnizori au oferit informații în cadrul răspunsurilor la chestionar despre incidentele petrecute în anul 2015. 12 furnizori au raportat că păstrează evidența incidentelor pe suport electronic, 6 furnizori atât pe suport fizic, cât și electronic și 6 furnizori păstrează evidența doar pe suport fizic. 4 furnizori nu au menționat metoda de păstrare a evidenței incidentelor.

Centralizatorul conține informații detaliate despre incidentele petrecute precum:	Nr. Respondenți
Impactul incidentului asupra proceselor afacerii, implicit asupra furnizării rețelelor și serviciilor de comunicații electronice	9
Momentele cheie ale incidentului (momentul producerii, detectării, încheierii incidentului etc.);	22

[7] Service Level Agreement

Cauza/cauzele ce au condus la producerea incidentului;	13
Locația incidentului (aria geografică afectată, dar și identificarea locației resurselor afectate);	22
Descrierea resurselor afectate;	13
Alte incidente/evenimente asociate/corelate;	7
Rezultatele evaluării incidentului;	10
Deciziile luate în vederea răspunsului la incident;	11
Acțiunile întreprinse în vederea remedierii incidentului/fluxul de lucru de la detectare până la remedierea incidentului;	19
Acțiunile planificate pentru recuperarea integrală în urma incidentului și pentru prevenirea altor incidente similare;	8
Comentarii ale personalului responsabil cu managementul incidentelor;	10
Informații de contact ale părților implicate – ale celui ce detectează/raportează incidentul și ale celui/celor ce se ocupă de tratarea acestuia;	12
Statusul incidentului în diferite etape/momente de timp pe tot parcursul desfășurării sale ce va fi actualizat după fiecare proces/activitate;	7
Cuantificarea costurilor implicate de rezolvarea incidentului;	2
Este actualizat ori de câte ori se înregistrează incidente.	15

În cazul a 16 dintre furnizori, sunt desemnate persoane responsabile cu colectarea informațiilor despre incidente și păstrarea evidenței.

Vulnerabilitățile sunt luate în considerare în cadrul procesului de colectare a informațiilor despre incidente și păstrarea evidenței acestora pentru 8 dintre furnizorii chestionați.

Printre activitățile asociate procesului de colectare a informațiilor despre incidente și păstrarea evidenței acestora, se regăsesc:

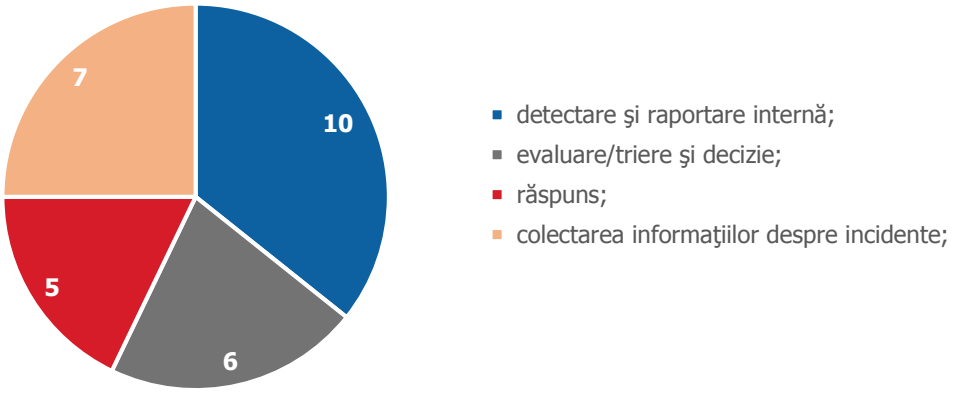
- completarea unor formulare de raportare a incidentelor;
- centralizarea informațiilor despre incidente;
- realizarea de rapoarte zilnice/lunare/săptămânale pentru incidentele din rețea;
- arhivarea informațiilor despre incidente.
- Unii furnizori colectează informații doar despre incidentele majore petrecute.
- Printre tipurile de incidente cel mai des întâlnite, furnizorii au menționat:
- fluctuații sau întreruperi ale alimentării cu energie electrică;
- incidente cauzate de fenomene naturale;
- secționarea cablurilor (datorită unor erori umane, pomi sau stâlpi căzuți sau furturilor);
- probleme software;
- echipamente defectate;
- viruși și furturi de identitate.

3.1.6 Automatizarea

În ceea ce privește automatizarea proceselor de management al incidentelor, 11 furnizori au raportat că există o automatizare a proceselor și 20 de furnizori au raportat că nu există procese automatizate în cadrul managementului incidentelor.

În figura 9 se pot observa tipurile de procese automatizate de furnizori.

Fig. 9 Procese automatizate



3.1.7 Incidente cibernetice

În cazul a 28 de furnizori, schema de management al incidentelor vizează și incidentele cibernetice. În figura 10 sunt prezentate tipurile de incidente cibernetice tratate de cei 28 de furnizori.

Fig. 10 Incidente cibernetice tratate

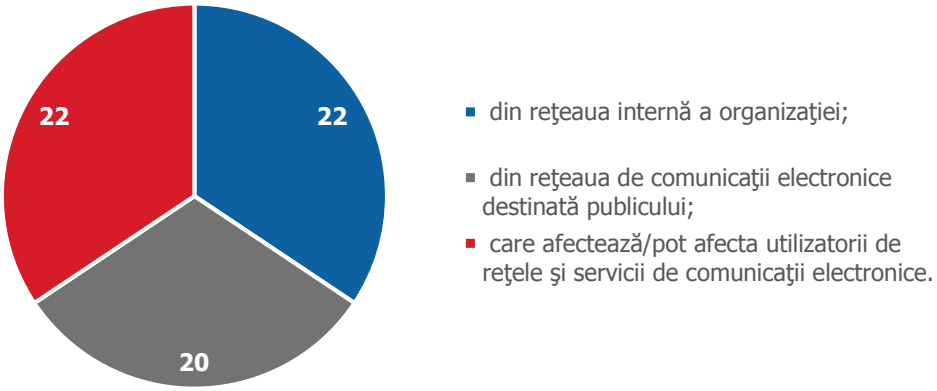
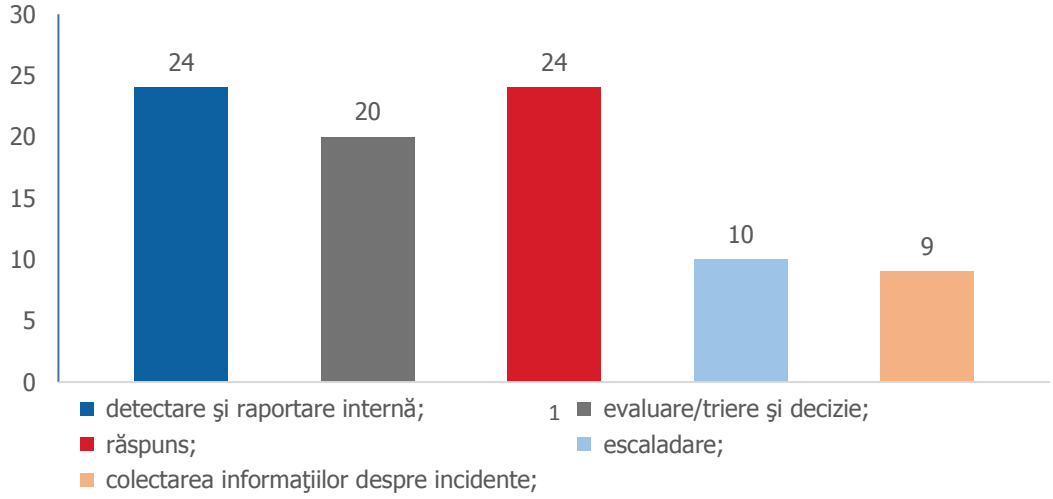


Fig. 11 În cazul incidentelor cibernetice schema de management al incidentelor cuprinde următoarele procese



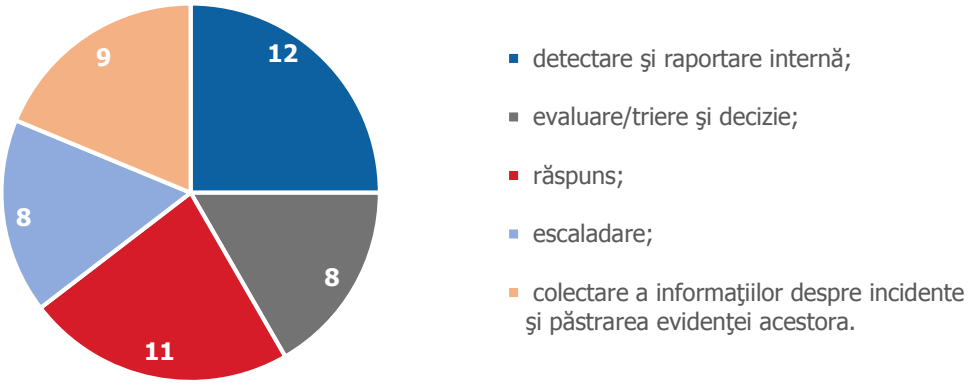
6 dintre furnizori au raportat că dețin o evidență a incidentelor cibernetice petrecute în anul 2015.

3.2 Proceduri corespunzătoare schemei de management al incidentelor

Procedurile documentate corespunzătoare managementului incidentelor vizează incidente ce afectează/pot afecta furnizarea rețelelor și serviciilor de comunicații electronice pentru 12 dintre furnizorii chestionați. Pentru 7 furnizori, procedurile vizează și incidentele cibernetice și numai în cazul a 3 furnizori, vizează și vulnerabilitățile detectate.

Procedurile privind managementul incidentelor acoperă procesele de detectare și raportare internă, evaluare/triere și decizie, răspuns, escaladare, colectare a informațiilor despre incidente și păstrarea evidenței acestora. Figura 12 prezintă răspunsurile furnizorilor în acest sens:

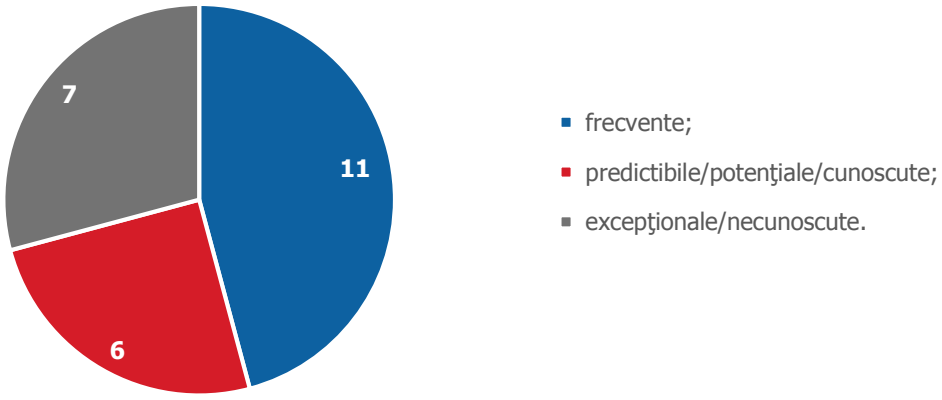
Fig. 12 Procese acoperite de procedurile privind managementul incidentelor



Procedurile privind managementul incidentelor cuprind și definirea, respectiv alocarea rolurilor și responsabilităților persoanelor adecvate pentru 9 furnizori.

În figura 13 sunt prezentate răspunsurile furnizorilor chestionați privind tipul de incidente acoperite de procedurile privind managementul incidentelor.

Fig. 13 Procedurile privind managementul incidentelor acoperă cazul incidentelor:



Doar în cazul a 2 furnizori procedurile privind managementul incidentelor cuprind definirea unor riscuri ce pot interveni pe parcursul desfășurării activităților aferente managementului incidentelor, cu precizarea modalităților în care se pot controla aceste riscuri.

4. Evaluarea schemei de management al incidentelor și îmbunătățiri

În vederea evaluării schemei de management al incidentelor, acumulării lecțiilor învățate și identificării îmbunătățirilor ce pot fi aduse măsurilor de securitate, 22 de furnizori au raportat că există mecanisme pentru a determina, măsura și monitoriza tipul și numărul incidentelor petrecute și dintre aceștia, doar 8 furnizori au raportat că există mecanisme pentru a determina, măsura și monitoriza costurile implicate în acțiunile de răspuns și/sau prevenire a unor incidente similare.

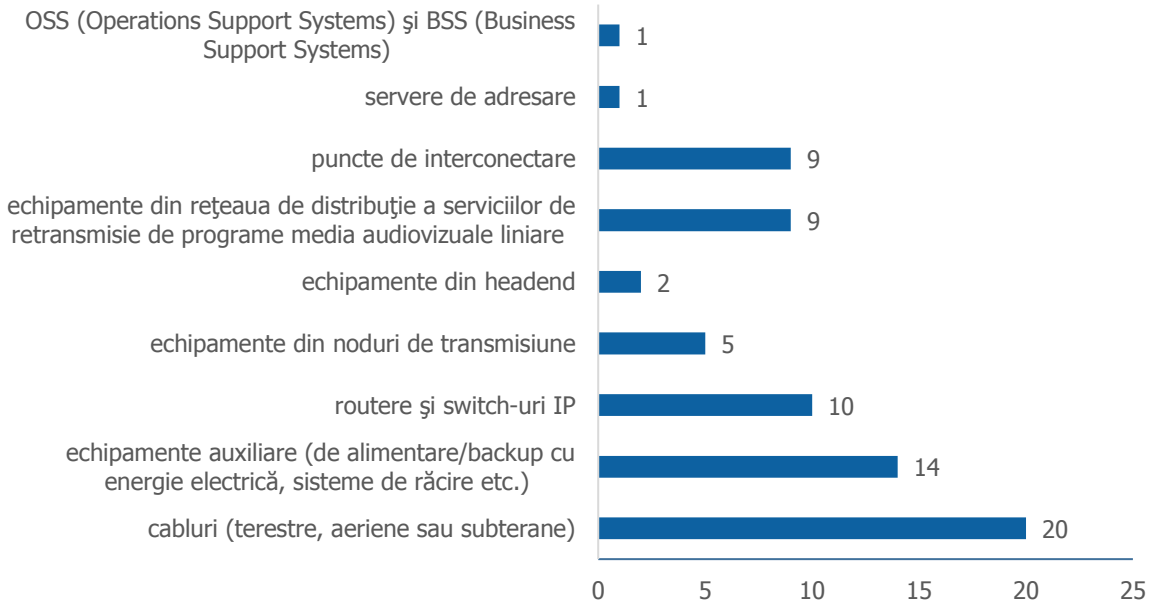
4.1 Analiza incidentelor și organizarea unor întâlniri

În ceea ce privește analiza informațiilor din centralizatorul incidentelor, 22 dintre furnizorii chestionați analizează periodic aceste informații pentru a identifica tendințele incidentelor și domeniile ce necesită atenție specială, pentru a identifica măsurile ce pot fi luate pentru prevenirea unor incidente similare și pentru a determina și corecta deficiențele proceselor și procedurilor de management al incidentelor. 7 dintre aceștia analizează periodic vulnerabilitățile. Totodată, 20 de furnizori organizează întâlniri de diseminare a informațiilor după incidentele majore, iar 18 furnizori organizează întâlniri periodice de diseminare a incidentelor. La aceste întâlniri, 21 dintre furnziori au raportat că participă atât personalul echipei de răspuns la incidente, cât și managementul organizației, doar 4 dintre aceștia afirmând că la întâlniri participă și alte persoane precum întregul personal tehnic, subcontractori, asociați și parteneri externi.

Doar 8 furnizori întocmesc rapoarte anuale interne privind incidentele înregistrate. Aceste rapoarte conțin numărul incidentelor înregistrate, tipul serviciilor de comunicații electronice afectate, numărul utilizatorilor sau conexiunilor afectate, acțiunile întreprinse pentru remediere, măsuri luate sau planificate pentru evitarea altor situații asemănătoare și durata soluționării diverselor tipuri de incidente, însă pentru nici unul dintre furnizori, rapoartele nu tratează și costurile implicate.

Furnizorilor li s-a solicitat să selecteze dintr-o listă de 19 categorii de resurse ce pot fi afectate de incidente, primele 3 categorii care sunt cel mai frecvent afectate. Astfel, cel mai frecvent afectate categorii de resurse sunt cablurile (terestre, aeriene sau subterane), echipamentele auxiliare (de alimentare/de backup cu energie electrică, sisteme de răcire etc.) și routere și switch-uri IP. Răspunsurile furnizorilor se pot observa în figura 14.

Fig. 14 Primele 3 categorii de resurse cel mai frecvent afectate de incidente în anul 2015

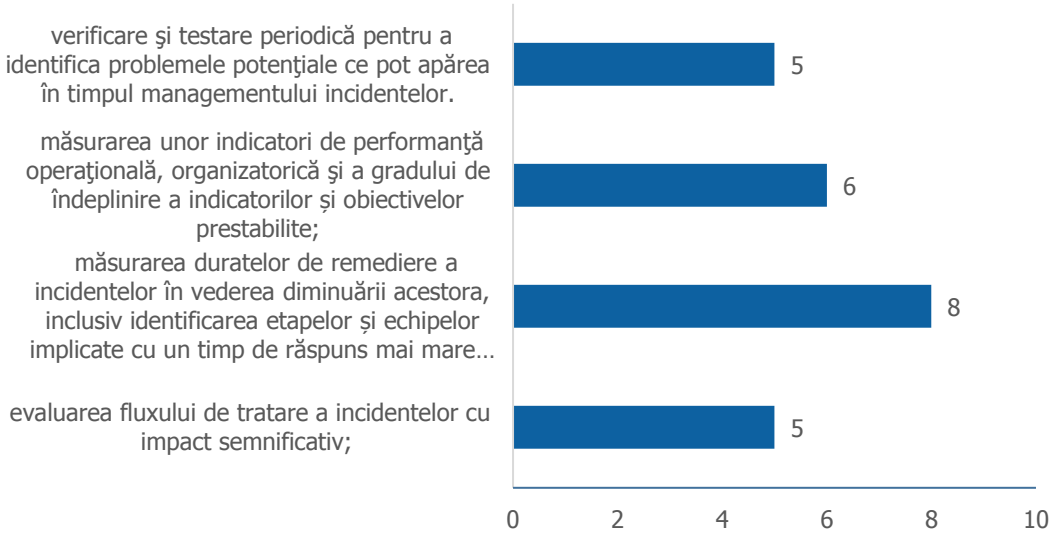


Printre rezultatele ultimei întâlniri periodice, în care s-au analizat incidentele din perioada anterioară, furnizorii au menționat măsuri precum instalare UPS-uri, schimbări tehnologice, înlocuire sau modificare de echipamente.

4.2 Evaluarea schemei de management al incidentelor

În ceea ce privește măsurarea periodică a eficacității proceselor și procedurilor de management al incidentelor, doar 9 dintre furnizori au raportat că realizează această măsurare. Metodele de măsurare a eficacității proceselor și procedurilor de management al incidentelor utilizate de cei 9 furnizori sunt ilustrate în figura 15.

Fig.15 Eficacitatea proceselor şi procedurilor de management al incidentelor este măsurată prin:



Nici unul dintre furnizori nu măsoară eficacitatea proceselor și procedurilor de management al incidentelor prin realizarea unor audituri interne SMSI[8] sau prin analize SMSI.

Printre rezultatele ultimei măsurări a eficacității proceselor și procedurilor de management al incidentelor menționate de furnizori, se regăsesc rezultate precum: scăderea numărului de incidente înregistrate anual, încadrarea în timpul asumat de rezolvare a incidentelor și necesitatea de verificări/reconstruiri/modernizări ale rețelelor de distribuție servicii în zonele cu incidente multiple.

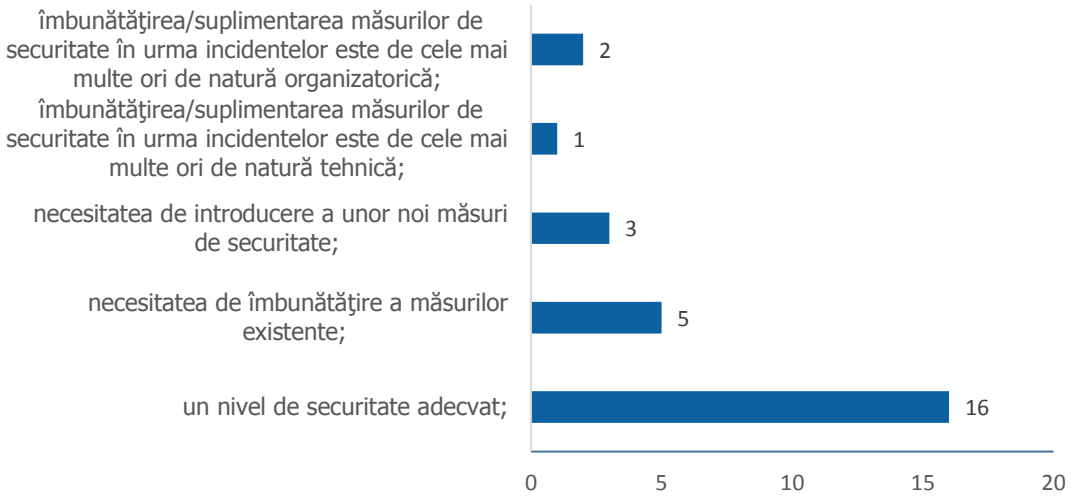
În urma măsurării eficacității proceselor și procedurilor de management al incidentelor din ultimul an, 2 dintre furnizori au menționat că au rezultat modificări asupra schemei de management al incidentelor, precum revizuirea stocurilor cu echipamente de rezervă sau simplificarea procesului de raportare a incidentelor către echipele de intervenție.

4.3 Îmbunătățiri ale măsurilor de securitate

Conform răspunsurilor primite de la furnizori, ultima analiză/evaluare a incidentelor și a schemei de management al incidentelor a scos în evidență aspectele prezentate în figura 16.

[8] SMSI - Sistem de Management al Securitatii Informatiei

Fig. 16 Rezultate în urma analizei/evaluării incidentelor și a schemei de management al incidentelor



Nici unul dintre furnizori nu a identificat vulnerabilități sau amenințări noi în urma analizei/evaluării incidentelor și a schemei de management al incidentelor.

Un singur furnizor documentează procesul de analiză/evaluare a incidentelor și a schemei de management al incidentelor și verifică și testează schimbările asupra proceselor și procedurilor de management al incidentelor.

II. Sistem de detectare a incidentelor

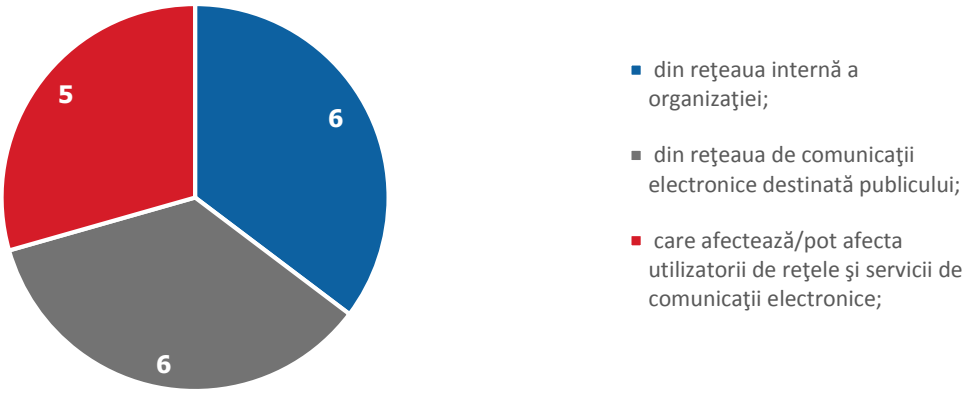
Conform Deciziei nr.512/2013, furnizorii au obligația să stabilească un sistem de detectare a incidentelor.

Procesele și procedurile din cadrul schemei de management al incidentelor trebuie să fie susținute de sisteme pentru detectarea, analiza, rezolvarea eficientă, în timp util a incidentelor care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

1. Sistem de detectare a incidentelor

Toți furnizorii chestionați dețin un sistem de detectare a evenimentelor/incidentelor care afectează sau pot afecta securitatea și integritatea rețelelor și serviciilor de comunicații electronice. Pentru 9 dintre aceștia, sistemul cuprinde capabilități și pentru detectarea incidentelor cibernetice, iar în cazul a 10 furnzori, incidentele cibernetice sunt detectate de către un sistem dedicat.

Fig. 17 Sistemul detectează incidentele cibernetice:



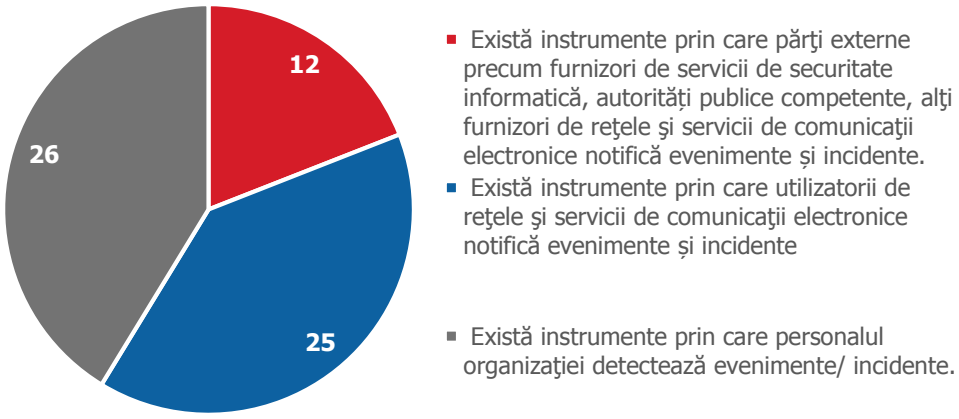
În urma detectării incidentelor și evenimentelor din diferite surse, 8 furnizori realizează o corelare a acestora.

Pentru 11 dintre furnizori, activitățile de detectare a incidentelor sunt realizate de către părți externe/organizații subcontractate.

1.1 Primirea sesizărilor și notificărilor despre incidente din partea unor persoane

Pentru cea mai mare parte a furnizorilor chestionați, evenimentele/incidentele ce pot afecta/afectează furnizarea rețelelor și serviciilor de comunicații electronice pot fi detectate și pe baza unor sesizări/informări din partea personalului organizației, din partea unor părți externe precum organizații de profil/parteneri de afaceri, altor furnizori de rețele și servicii de comunicații electronice, precum și din partea utilizatorilor de rețele și servicii de comunicații electronice.

Fig. 18 Instrumente prin care se primesc sesizări și notificări despre incidente



Printre instrumentele utilizate de către furnizori prin care se primesc sesizări și notificări despre incidente din partea unor persoane, se numără comunicarea directă/verbală, e-mail, fax, telefon, prin intermediul alarmelor, call center, folosind platforme de *ticketing* pentru înregistrarea incidentelor/deschiderea unor sesizări, prin informarea *NOC*-ului, a turelor de monitorizare a funcționării sistemelor, a șefului direct.

1.2 Sisteme de monitorizare automată

Se pot utiliza sisteme, soluții și platforme menite să asigure monitorizarea optimă a elementelor rețelei de comunicații electronice, a rețelei interne, a locațiilor și a mediului în vederea detectării oricărui eveniment care poate afecta furnizarea rețelelor și serviciilor de comunicații electronice.

1.2.1 Monitorizarea rețelelor și serviciilor de comunicații electronice

În cadrul organizației trebuie să existe procese și activități de monitorizare, analiză și control al funcționării optime a rețelei de comunicații electronice. Detectarea evenimentelor, incidentelor și vulnerabilităților se poate realiza automat, pe baza primirii unor informații de la echipamente și sisteme, sub forma unor alerte, notificări, rapoarte etc.

În cazul a 24 de furnizori, există sisteme, soluții și platforme utilizate pentru monitorizarea elementelor rețelei de comunicații electronice. În figura 19 se poate observa cum se realizează monitorizarea rețelei de comunicații electronice.

Fig. 19 Monitorizarea rețelei

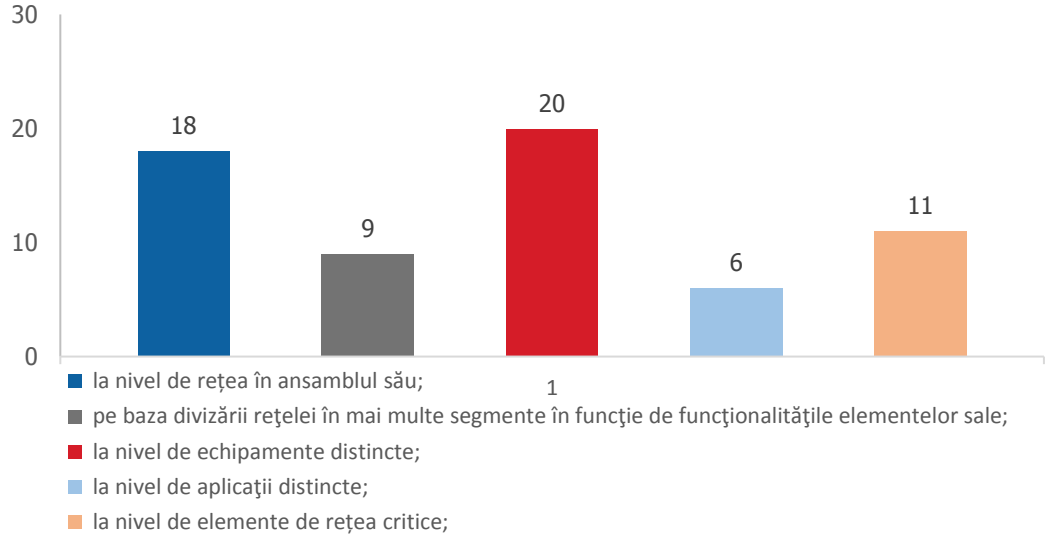
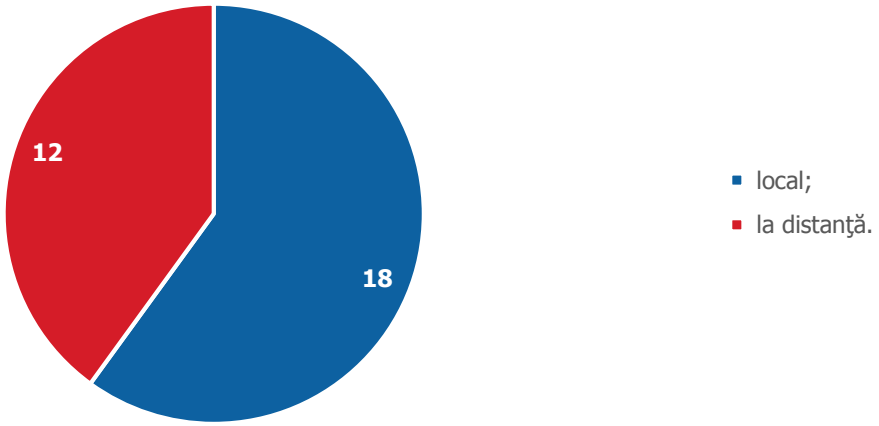
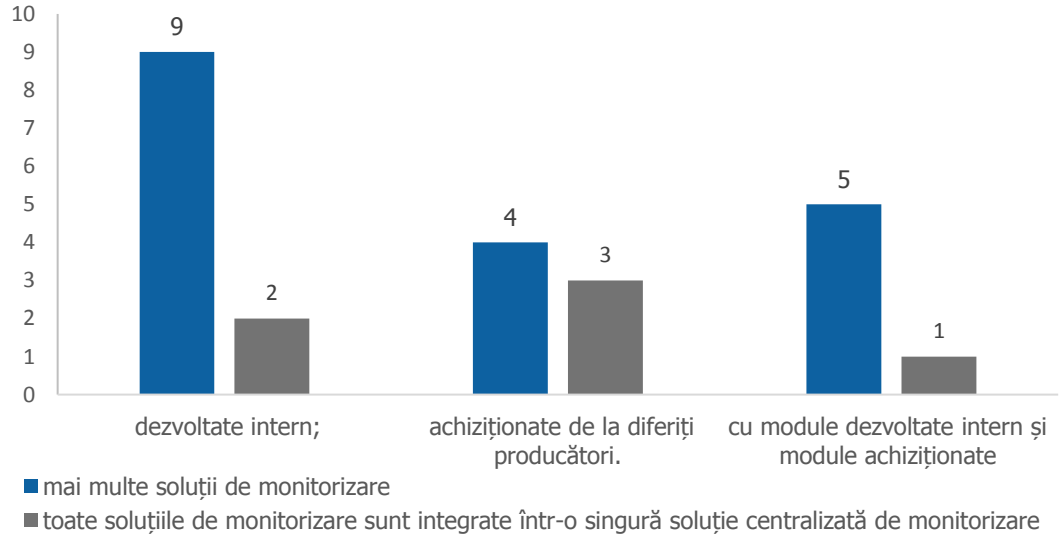


Fig. 20 Monitorizarea se realizează:



24 de furnizori au raportat că monitorizarea rețelei și serviciilor de comunicații electronice este realizată cu ajutorul unor sisteme, platforme și aplicații specifice dedicate (fig.21).

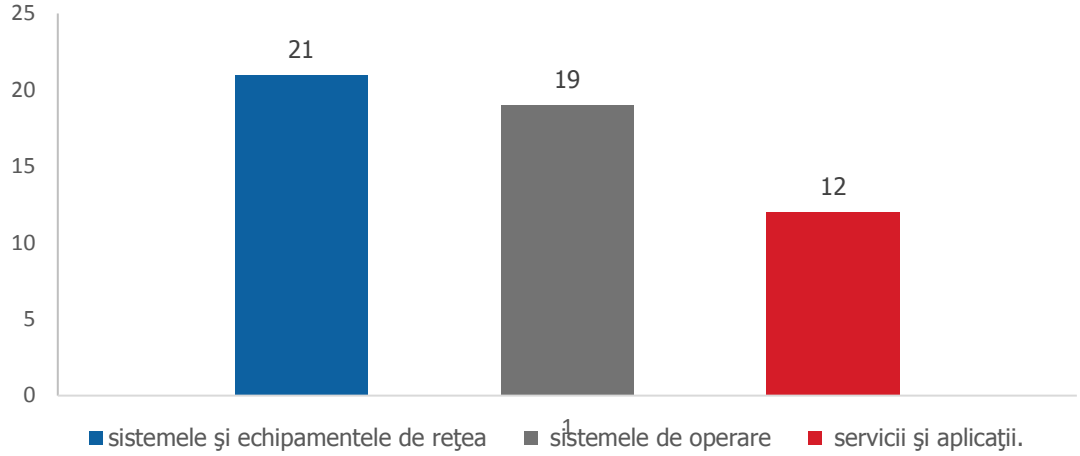
Fig. 21 Soluția privind monitorizarea rețelei și serviciilor



În cazul a 15 dintre furnizorii respondenți, sunt stabiliți parametri și praguri predefinite la atingerea cărora sistemul/sistemele de monitorizare generează alerte, notificări și rapoarte.

Figura 22 prezintă sursa logurilor analizate de către sistemele de monitorizare ale furnizorilor.

Fig. 22 Se analizează loguri generate de:



Printre sistemele de monitorizare utilizate în cadrul organizațiilor furnizorilor au fost menționate: Wanguard, Cacti, Nagios, monitorizare GPS a echipelor de răspuns, SNMPC, NMS2, RADIUS, ITMS, CRM, Zoho Operations Manager.

1.2.2 Monitorizarea rețelei interne

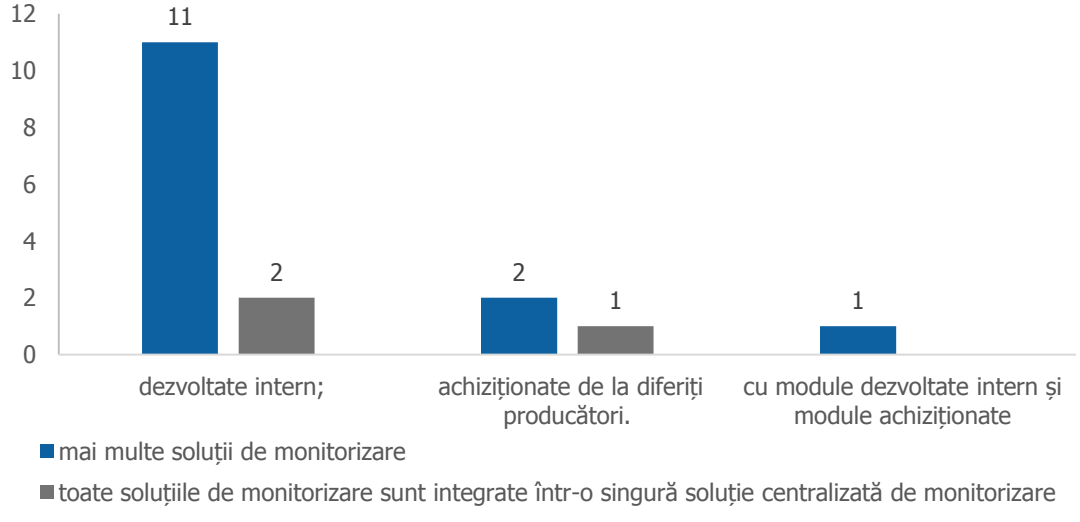
19 furnizori au raportat că monitorizează rețeaua internă.

Majoritatea răspunsurilor la întrebarea dedicată descrierii procesului/modalităților de monitorizare a rețelei interne a organizației au fost concentrate pe soluții de monitorizare specifice (de exemplu aplicație software dedicată cu alertare în cazul incidentelor, soluție integrată de monitorizare, *gateway* prin care este administrată rețeaua internă, soft-uri de management dedicate).

Răspunsurile au indicat faptul că nu au existat cazuri în care afectarea/compromiterea rețelei interne să conducă la afectarea furnizării rețelelor și serviciilor de comunicații electronice.

În cazul a doi furnizori, soluțiile de monitorizare a rețelei interne sunt separate de soluțiile de monitorizare a rețelei de comunicații electronice.

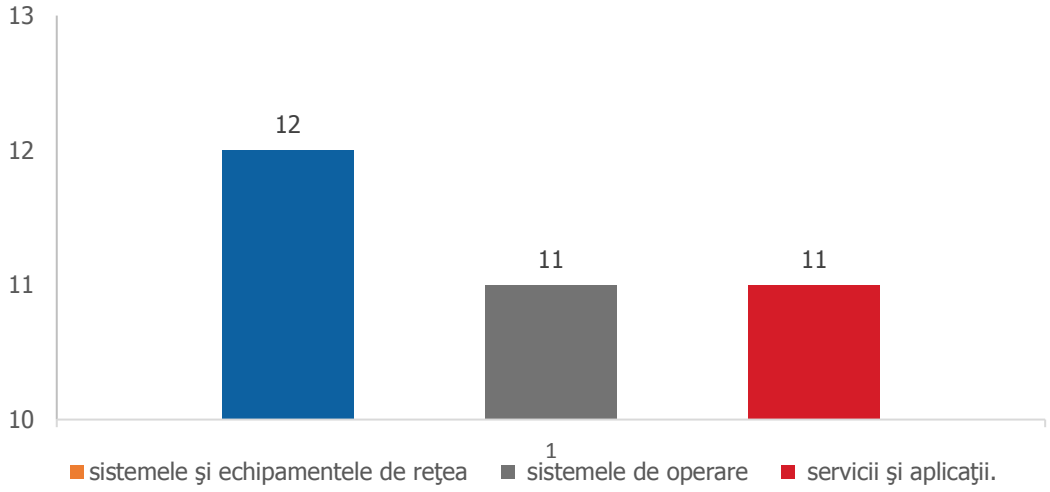
Fig. 23 Soluțiile de monitorizare a rețelei interne



12 dintre furnizori dețin parametri și praguri predefinite la atingerea cărora sistemul/sistemele de monitorizare generează alerte, notificări și rapoarte.

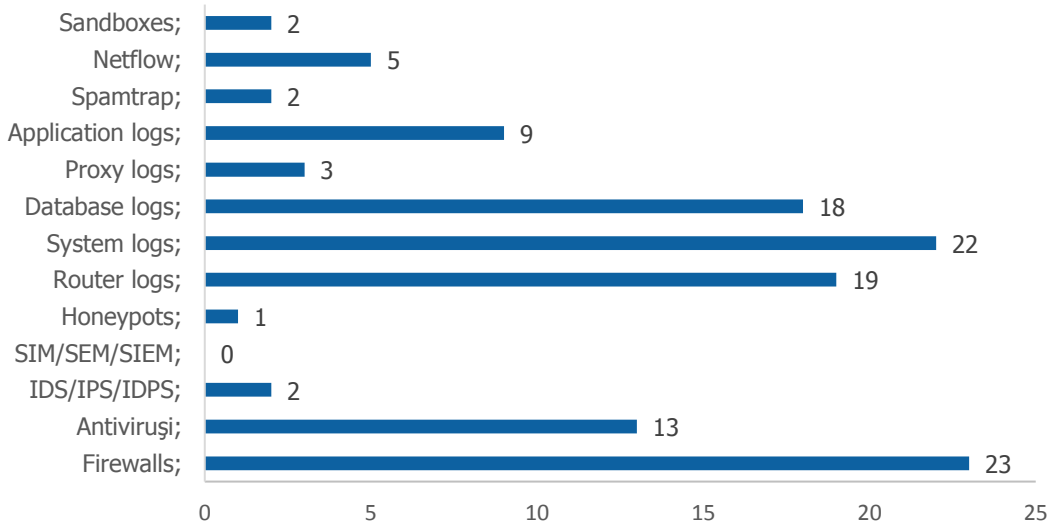
Figura 24 prezintă sursa logurilor analizate de către sistemele de monitorizare ale furnizorilor în ceea ce privește rețeaua internă.

Fig. 24 Se analizează loguri generate de:



Furnizorii au fost rugați să bifeze situațiile aplicabile în ceea ce privește sistemele/instrumentele de detectare din cadrul propriilor organizații și utilizarea acestora. Răspunsurile sunt ilustrate în figura 25.

Fig. 25 Sisteme de monitorizare a rețelei interne utilizate de către furnizori



Așa cum se observă și din graficul anterior, majoritatea furnizorilor utilizează *firewalls* și înregistrări la nivel de echipament de rutare, sistem, bază de date, aplicație *(router logs, system logs, database logs)* pentru detectarea evenimentelor/incidentelor. Interesul cel mai scăzut aparține unor sisteme/instrumente precum *honeypots, sandboxes, spamtrap, IDS/IPS/IDPS și SIM/SEM/SIEM*.

Printre incidentele care au afectat rețeaua internă în anul 2015, furnizorii au menționat întreruperi în alimentarea cu energie electrică, defecțiuni ale unor cabluri, servere sau switch-uri, viruși și atacuri de tip *DDOS*.

1.2.3 Monitorizarea accesului în locații

Răspunsurile la chestionar indică existența unor sisteme de detectare a incidentelor cauzate de accesul neautorizat în cazul a 24 de furnizori. Figura 26 arată tipul zonelor monitorizate de către furnizori împotriva accesului neautorizat.

Fig. 26 Există sisteme de detectare a incidentelor cauzate de accesul neautorizat în:

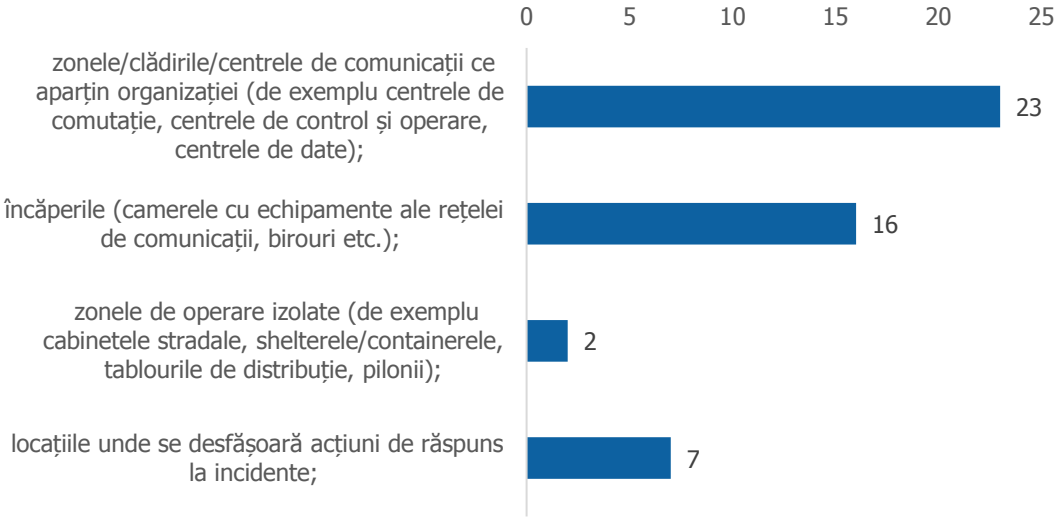
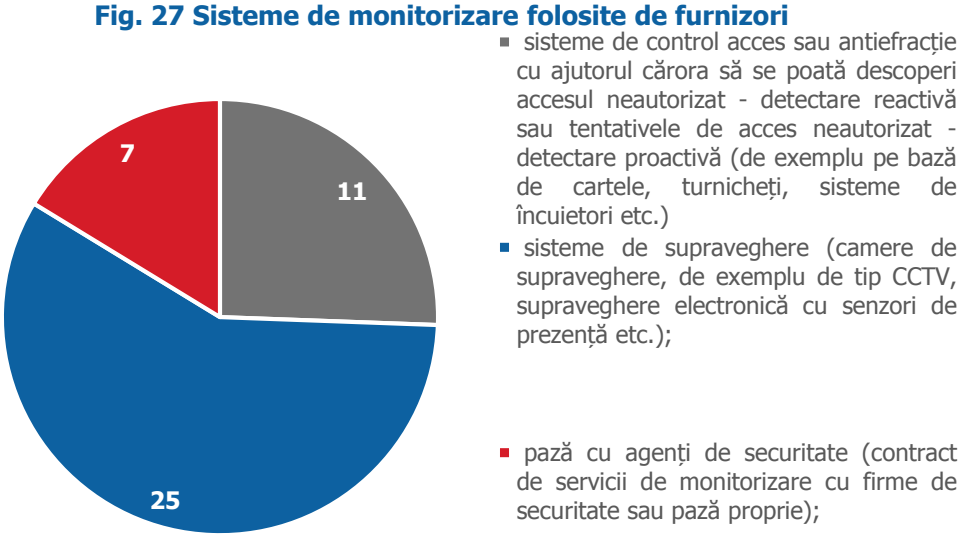


Figura 27 prezintă sistemele de detectare a incidentelor cauzate de accesul neautorizat în interiorul zonelor/clădirilor/centrelor de comunicații menționate de furnizori.

Fig. 27 Sisteme de monitorizare folosite de furnizori



Din răspunsurile furnizorilor se poate observa că cel mai utilizate sisteme de detectare a incidentelor cauzate de accesul neautorizat sunt sistemele de supraveghere, precum camere de supraveghere, supraveghere pe bază de senzori etc.

1.2.4 Monitorizarea mediului

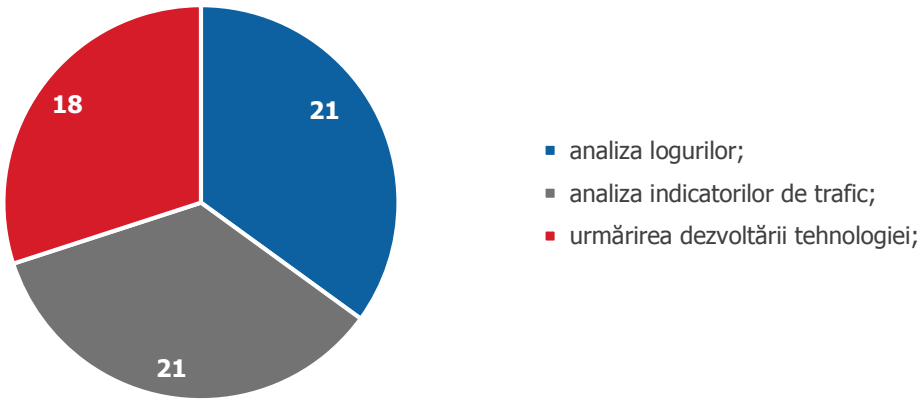
În cazul a 10 furnizori, sunt utilizate sisteme de detectare, alarmare și alertare adecvate pentru a reduce efectele dezastruoase ale apariției unor incidente severe cauzate de incendii, inundații, cutremure, explozii și alte forme de dezastre naturale sau provocate de oameni.

Potrivit răspunsurilor furnizorilor, printre condițiile de mediu monitorizate se regăsesc temperatura, focul, fumul, umiditatea și gazele, iar sistemele cu ajutorul cărora se realizează monitorizarea sunt bazate pe senzori.

1.3. Detectare proactivă

21 de furnizori au raportat că organizația deține sisteme pentru detectarea proactivă a evenimentelor, incidentelor și vulnerabilităților. Figura 28 prezintă răspândirea unor sisteme pentru detectarea proactivă în rândul furnizorilor.

Fig. 28 Siseme pentru determinarea proactiva

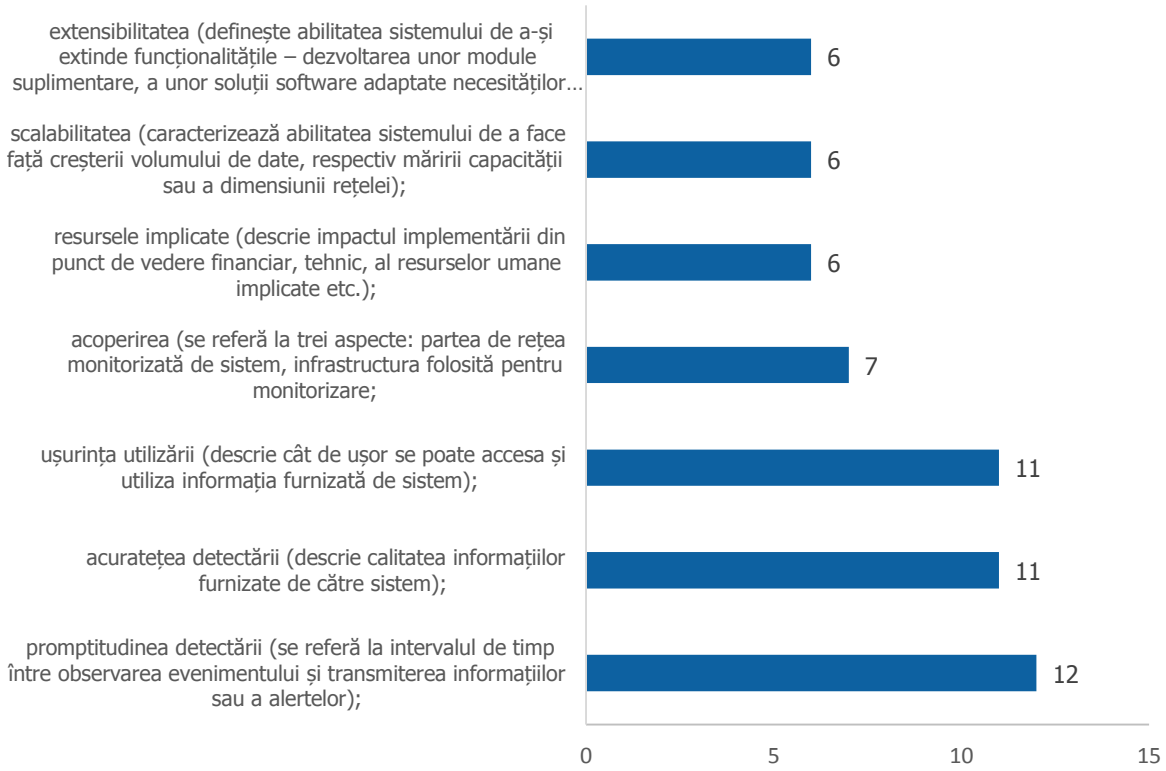


2. Evaluarea și actualizarea sistemului de detectare

Sistemul de detectare a incidentelor este evaluat și actualizat periodic și ori de câte ori este nevoie în cazul a 22 de furnizori.

În cazul a 20 de furnizori, actualizarea sistemelor de detectare ține cont de schimbările înregistrate în cadrul rețelei și de incidentele petrecute. 13 furnizori actualizează sistemele de detectare ținând cont de modificările asupra proceselor afacerii.

Fig. 29 Sistemele pentru detectarea incidentelor sunt evaluate pe baza următoarelor criterii:



Printre îmbunătățirile aduse sistemelor de detectare a incidentelor, ca urmare a ultimei evaluări a acestora, furnizorii au menționat îmbunătățiri precum:

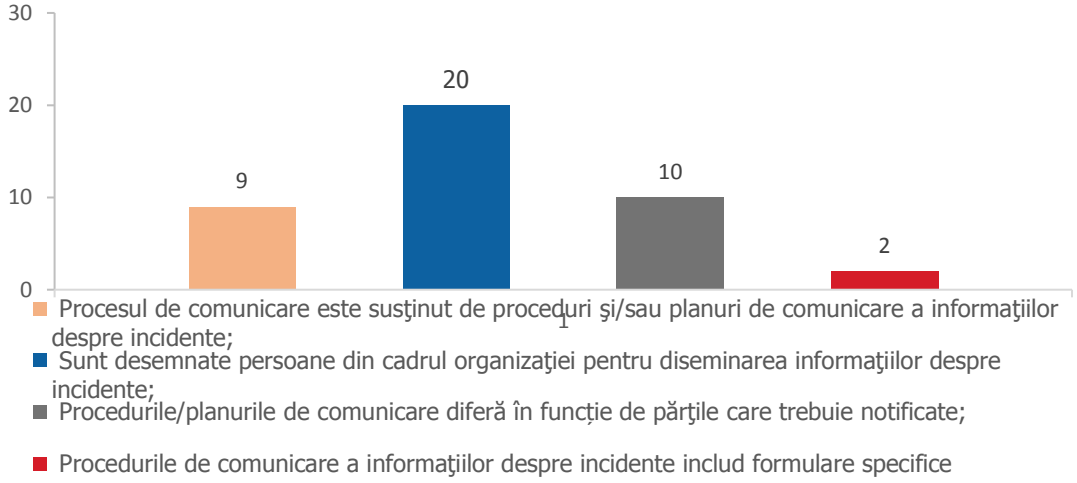
- trecerea de la IP public la IP privat;
- upgrade-uri hardware și software;
- introducerea unor noi caracteristici precum alertare prin SMS;
- instalarea unor sisteme noi de detecție a fumului și focului;
- instalarea camerelor de supraveghere.

III. Proceduri și planuri de comunicare a incidentelor

Conform Deciziei nr.512/2013, furnizorii au obligația să stabilească o procedură adecvată de raportare a incidentelor către ANCOM, precum și către alte autorități responsabile și să stabilească planuri de comunicare a incidentelor către alte părți externe (furnizori de rețele și servicii de comunicatii electronice afectati, media, clienti, parteneri de afaceri etc.).

În ceea ce privește procedurile și planurile de comunicare a informațiilor despre incidente, 22 de furnizori au afirmat că dețin un proces privind comunicarea informațiilor despre incidente unor părți externe. Procesul de comunicare este susținut de proceduri și/sau planuri de comunicare a informațiilor despre incidente pentru 9 furnizori. Procedurile de comunicare a informațiilor despre incidente includ formulare specifice pentru 2 furnizori. Aspecte despre aceste proceduri și planuri sunt prezentate grafic în figura 30 pentru cei 22 de furnizori.

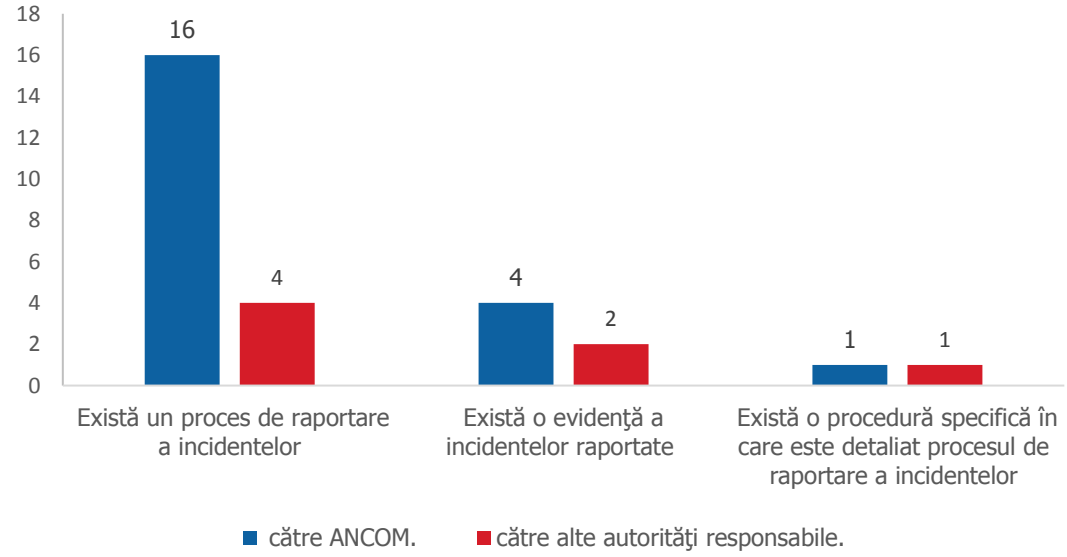
Fig. 30 Proceduri și planuri de comunicare a incidentelor



1. Proceduri de raportare a incidentelor către ANCOM, precum și către alte autorități responsabile

Potrivit răspunsurilor oferite, 16 furnizori au un proces de raportare a incidentelor către ANCOM, însă doar un furnizor deține proceduri specifice în care este detaliat acest proces și 4 furnizori păstrează o evidență a incidentelor raportate către ANCOM.

Fig. 31 Procesul de raportare a incidentelor

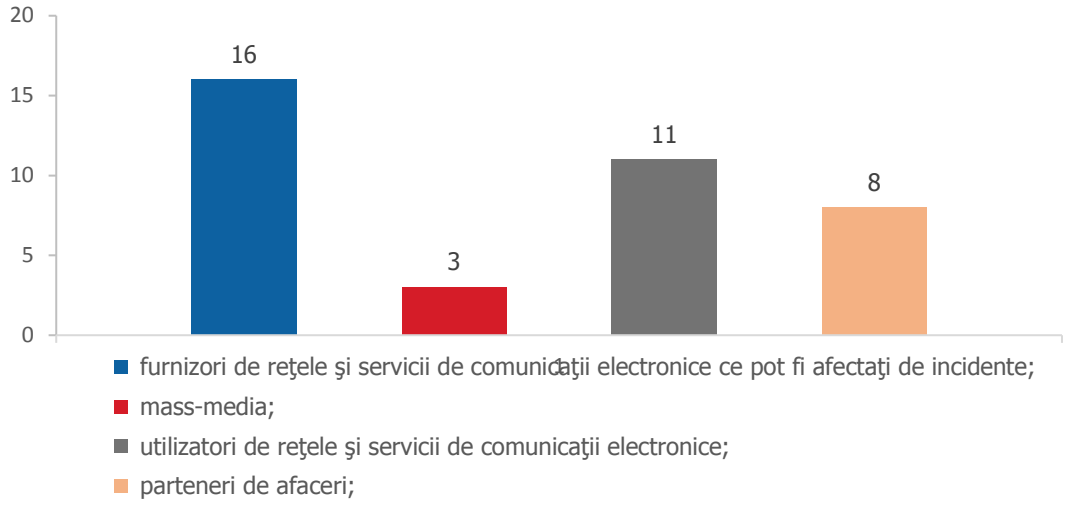


În afară de ANCOM, 4 furnizori au menționat că transmit informații despre incidente și altor autorități/instituții precum Poliție, SRI, CNA, IGPR.

2. Planuri de comunicare către alte părți

Figura 32 arată în ce proporție există planuri de comunicare a incidentelor către diferite grupuri de interes în rândul celor chestionați.

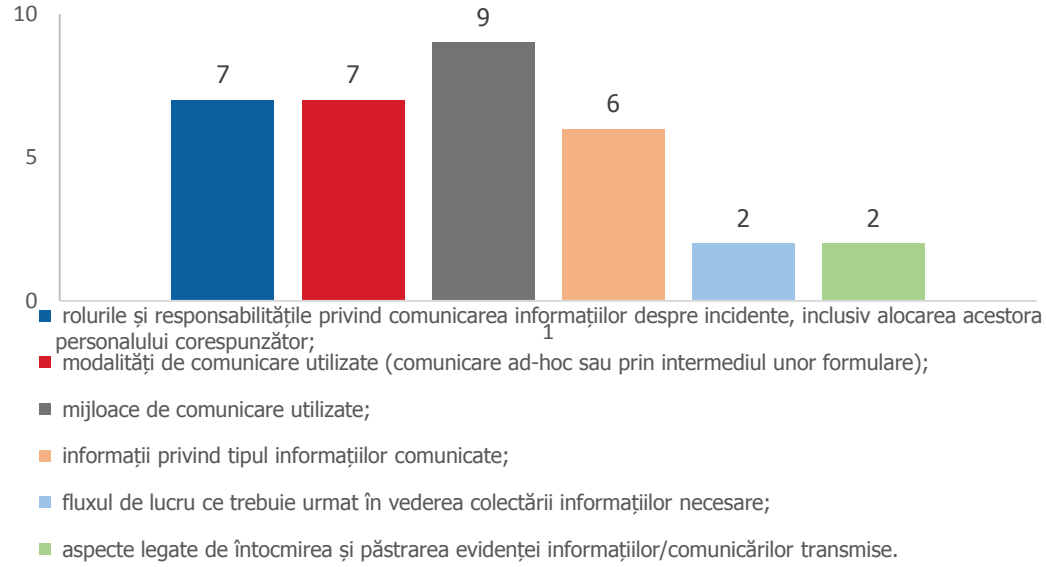
Fig. 32 Există planuri de comunicare a incidentelor către:



Comunicarea cu părțile prezentate în figura 32 se face prin telefon, email, fax, SMS, comunicat de presă sau anunț pe posturile tv/radio local.

Figura 33 prezintă situația în rândul respondenților în ceea ce privește elementele conținute de planurile privind comunicarea informațiilor despre incidente unor părți externe organizației.

Fig. 33 Planurile privind comunicarea informaţiilor despre incidente unor părţi externe organizaţiei conţin

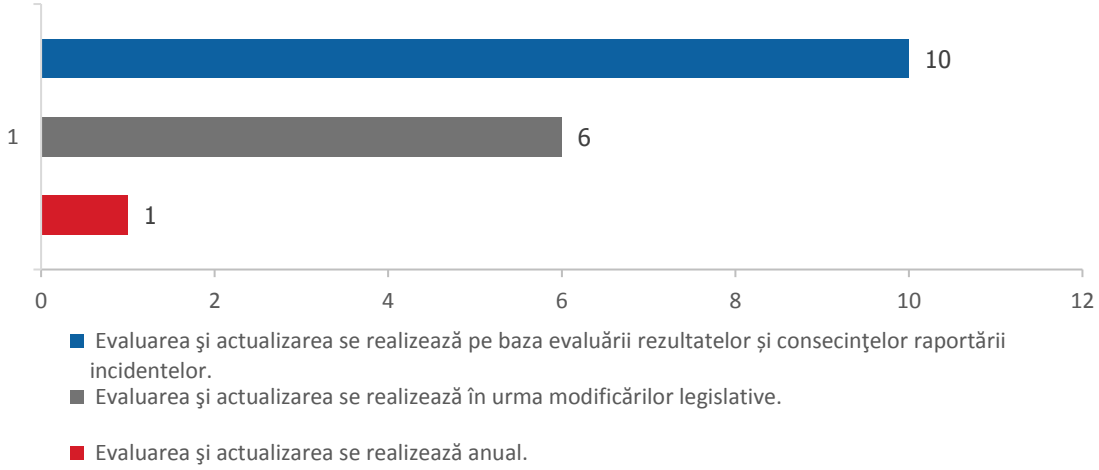


În cazul a 3 furnizori, informațiile de interes pentru public în ceea ce privește incidentele petrecute se publică și în cazul a 7 furnizori, unele informații despre incidente sunt comunicate nestandardizat, prin metode alese în funcție de circumstanțele incidentului (comunicare ad-hoc).

3. Evaluarea și actualizarea planurilor și procedurilor de comunicare sau raportare a incidentelor

Evaluarea și actualizarea planurilor și procedurilor de comunicare sau raportare a incidentelor este realizată de doar 10 dintre furnizorii respondenți. Figura 34 se referă la procesul de evaluare și actualizare a procedurilor și planurilor privind comunicarea sau raportarea informațiilor despre incidente unor părți externe.

Fig. 34 Evaluarea şi actualizarea planurilor şi procedurilor de comunicare sau raportare a incidentelor



Nu există indicatori de monitorizare și evaluare a procesului de comunicare externă pentru măsurarea eficienței, în cazul nici unui furnizor respondent.

IV. Alte informații

1. Tipurile de incidente care sunt cel mai greu de detectat și remediat

a) Printre tipurile de incidente cel mai greu de detectat, furnizorii au menționat:

- incidentele cauzate de erori software;
- decopertarea și identificarea exactă a segmentului de fibră optică subterană secționată;
- incidentele care nu generează alarme, performanțele serviciului fiind în parametrii normali;
- incidentele de rutare, caz în care izolarea ariei de impact este mai dificil de realizat;
- atacurile de tip *DDoS* orientate către mai multe destinații cu scopul congestionării rețelei;
- incidentele referitoare la vulnerabilități de tip *zero-day*;
- probleme întâmpinate în retransmisia programelor audiovizuale;
- erorile de configurație care nu sunt evidente, dar care afectează buna funcționare a echipamentelor;
- reclamațiile de la clienți care nu conțin informații necesare identificării cauzei.

b) Printre incidentele cel mai greu de remediat, furnizorii au menționat:

- incidente cauzate de erori software;
- incidente cauzate de secționarea fibrei optice situate subteran;
- atacuri de tip DDoS orientate către mai multe destinații cu scopul congestionării rețelei;
- incidente care afectează echipamente fără update de firmware;
- incidente cibernetice;
- incidente care presupun acces fizic la locație;
- incidente care implică resurse ce nu sunt sub controlul furnizorului;
- incidente produse în locații izolate;

- incidente cauzate de condiții meteorologice nefavorabile;
- incidente ce necesită intervenția unor echipe suplimentare, eventual din afara organizației, în vederea soluționării.

2. Probleme frecvente cu care se confruntă furnizorii

a) Printre problemele frecvente cu care se confruntă furnizorii în privința detectării și raportării evenimentelor, incidentelor și vulnerabilităților, se regăsesc:

- resursele umane greu de instruit;
- colaborarea între diferite părți;
- erori umane;
- lipsa de informații privind unele incidente cibernetice.

b) Printre problemele frecvente cu care se confruntă furnizorii în privința analizei, evaluării și trierii incidentelor, se regăsesc:

- resursele umane insuficient pregătite;
- timp și resurse umane limitate;
- erorile umane;
- incidentele multiple cauzate de fenomene naturale.

c) Printre problemele frecvente cu care se confruntă furnizorii în privința răspunsului la incidente, inclusiv escaladarea, se regăsesc:

- situațiile în care este atribuită unui incident o echipă de răspuns care nu este abilitată să rezolve respectivul incident în mod direct;
- indisponibilitatea echipei în cazul incidentelor multiple;
- incidentele cauzate de fenomene naturale care împiedică accesul la locația incidentului.

d) Printre problemele frecvente cu care se confruntă furnizorii în privința colectării informațiilor despre incidente și păstrării evidenței acestora, se regăsesc:

- informații insuficiente despre incident;
- colectarea informațiilor și păstrarea evidenței pe suport fizic;
- resursele umane limitate;
- timpul limitat;
- lipsa unei aplicații care să centralizeze toate informațiile despre evenimente/incidente/vulnerabilități.

e) Printre problemele frecvente cu care se confruntă furnizorii în privința comunicării informațiilor despre incidente unor părți externe, se regăsesc:

- inexistența unor formulare standardizate pentru comunicare;
- imposibilitatea automatizării procesului de comunicare;
- colaborarea dificilă cu anumite părți;
- timpul limitat.

3. Standardele/recomandările sau alte documente/publicații de standardizare europene și/sau internaționale utilizate de furnizori pentru implementarea unor măsuri în domeniul managementului incidentelor

Printre standardele menționate de furnizori se regăsesc:

- ISO 27001
- ISO 27002

- ISO 27011
- ITIL
- ISO 27035

4. În privința certificărilor, nici unul dintre furnizorii respondenți nu a raportat că deține certificări în domeniul Managementul incidentelor.

5. Incidente înregistrate de furnizori în anul 2015

28 de furnizori au afirmat că există facilități/sisteme/instrumente tehnice și operaționale de colectare a informațiilor despre evenimente/incidente și țin o evidență a incidentelor petrecute în cadrul propriilor organizații pe suport fizic sau/și electronic. Dintre aceștia, 23 de furnizori au oferit informații în cadrul răspunsului la chestionar despre incidentele petrecute în anul 2015.

Furnizorii respondenți au declarat un număr total de 35.383 de incidente petrecute și înregistrate în 2015, cu o medie de 1.538 de incidente per furnizor. Figura 35 ilustrează numărul de incidente total raportat de cei 23 de furnizori în funcție de localizarea acestora în cadrul rețelei de comunicații electronice. Menționăm că numărul de incidente raportate de fiecare furnizor variază foarte mult, anumiți furnizori detectând un număr mare de incidente, iar alții înregistrând doar câteva.

Fig. 35 Care este numărul total de incidente care au afectat:

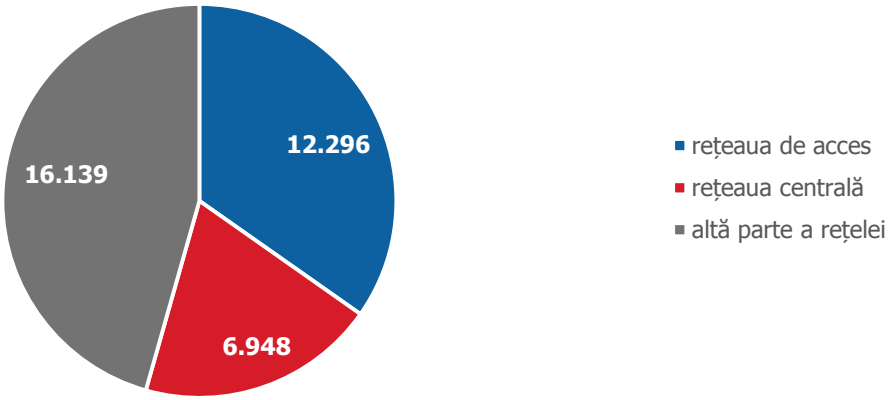
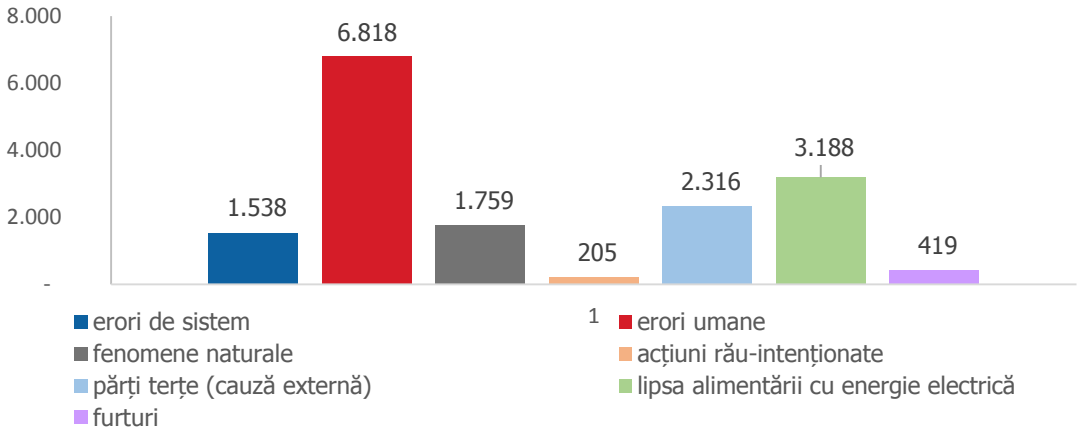


Figura 36 prezintă numărul total de incidente raportate de furnizori în cadrul răspunsului la chestionar, în funcție de cauza acestora. Câțiva dintre furnizori nu au oferit informații și despre numărul total de incidente înregistrate în 2015 în funcție de cauză.

Fig. 36 Numărul total de incidente cauzate de



9 furnizori au oferit informații privind incidentele cibernetice înregistrate în 2015. Numărul total al acestora este de 3.992, cu o medie de 444 de incidente per furnizor. Și în cazul acestor incidente se observă o diferență între numărul de incidente înregistrate de fiecare dintre cei 9 furnizori respondenți.

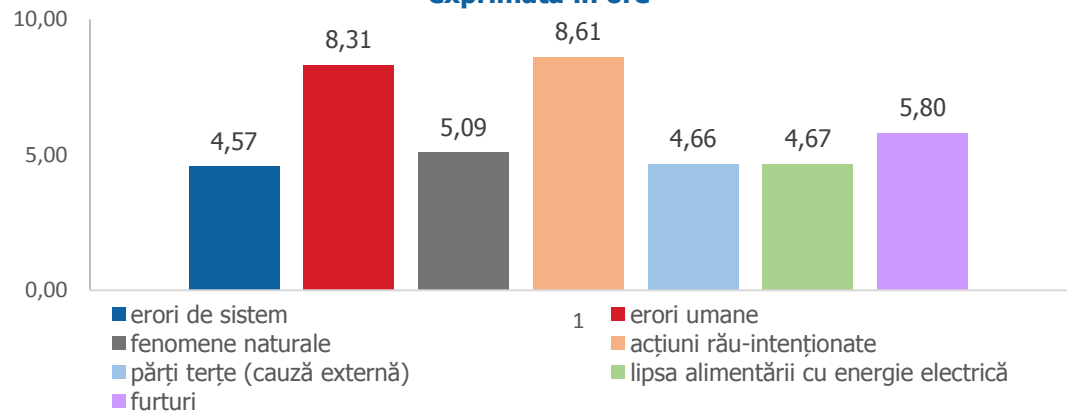
În ceea ce privește evaluarea impactului incidentelor, 17 furnizori au prezentat informații legate de modul cum evaluează impactul și câte incidente se încadrează în categoriile de incidente cu impact mic, mediu și mare. Astfel, cei mai mulți furnizori evaluează impactul unui incident în funcție de numărul de abonați/clienți sau conexiuni afectate de acel incident și folosesc praguri precum:

- impact mic: incidente care afectează până la 5, 10, 200 sau 500 de conexiuni.
- impact mediu: incidente care afectează un număr de conexiuni între 5 și 20, între 10 și 20, între 50 și 200, între 50 și 500 și între 500 și 1000.
- impact mare: incidente care afectează mai mult de 20, 50 200, 500 sau 1000 de conexiuni.

Alți parametri utilizați de furnizori pentru a estima impactul (mic, mediu sau mare) sunt: număr de canale TV ce nu se recepționează la clienți, număr de noduri de rețea, POP-uri nefuncționale, număr de localități afectate sau afectarea unor echipamente principale predefinite (switch-uri, routere sau tronsoane de fibră optică).

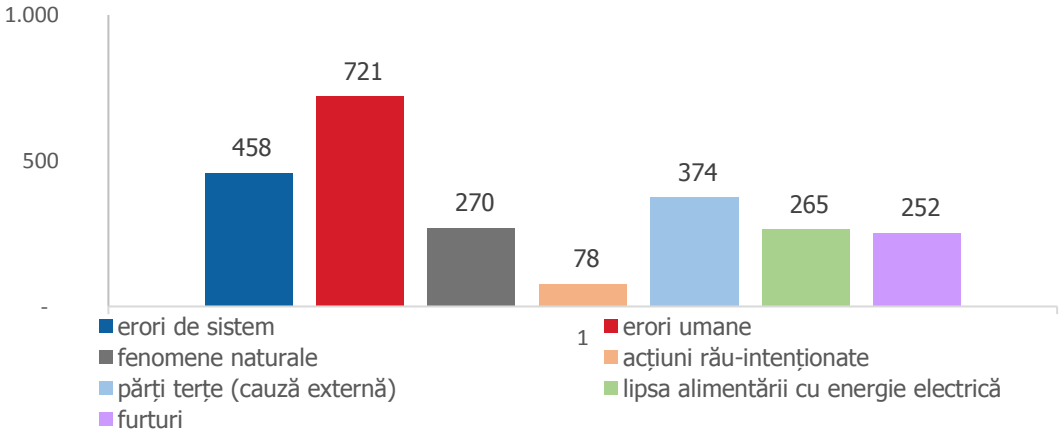
Durata medie a incidentelor raportate de furnizori în cadrul răspunsului la chestionar pentru anul 2015 este de 4,32 ore. În figura 37 se pot observa duratele medii ale incidentelor în funcție de cauzele acestora.

Fig. 37 Durata medie a incidentelor per categorie de cauze exprimată în ore



Numărul mediu de conexiuni afectate calculat pentru cei 18 furnizori care au oferit informații este de 1.126 de conexiuni. În figura 38 se pot observa numărul mediu de conexiuni raportat de furnizori în funcție de cauză. Menționăm faptul că nu toți cei 18 furnizori care au oferit informații privind numărul mediu de conexiuni afectate de un incident au furnizat informații și despre durata medie a unui incident per categorie de cauză.

Fig. 38 Număr mediu de conexiuni afectate per cauză



V. Concluzii

Prezentul raport tratează managementul incidentelor din perspectiva măsurilor de securitate pe care furnizorii trebuie să le implementeze în vederea asigurării securității și integrității rețelelor și serviciilor de comunicații electronice, conform obligațiilor legale: stabilirea de procese și proceduri pentru managementul incidentelor, sisteme de detectare a incidentelor, proceduri și planuri de comunicare a incidentelor.

Raportul reflectă abordările și practicile celor 31 de furnizori chestionați în ceea ce privește managementul incidentelor. Prin intermediul acestuia, ANCOM își propune să sprijine furnizorii chestionați prin diseminarea informațiilor referitoare la bunele practici existente în domeniul managementului incidentelor, așa cum rezultă din răspunsurile oferite la chestionar.

În urma centralizării și analizei răspunsurilor la chestionar se pot desprinde următoarele concluzii:

1. Managementul incidentelor
    - 50% din furnizorii chestionați au o politică de management al incidentelor;
    - 100% din furnizorii chestionați au o echipă care se ocupă cu managementul incidentelor;
    - În cazul a 19 furnizori (61%) echipele de răspuns la incidente sunt disponibile în timp real, 24/7;
    - Serviciul de management al incidentelor este total externalizat în cazul a 2 furnizori (6,5%) și parțial externalizat în cazul a 11 furnizori (35,5%).

2. Servicii acoperite de furnizori
    - 31 de furnizori se axează pe servicii reactive (100%);
    - 24 de furnizori realizează și servicii proactive (77%);
    - 18 furnizori realizează și servicii privind managementul calității și securității (58%).

3. Schema de management al incidentelor

100% dintre furnizori declară că dețin o schemă de management al incidentelor mai mult sau mai puțin dezvoltată și care tratează toate procesele sau doar o parte din acestea:

- Detectare - 31 de furnizori (100%);
- Evaluare - 27 de furnizori (87%);
- Corelare - 26 de furnizori (83,9%);
- Răspuns - 31 de furnizori (100%);
- Escaladare - 15 furnizori (48,4%);
- Colectare - 28 de furnizori (90,3%);
- Există procese automatizate în cazul a 11 furnizori (35,5%).

4. Proceduri corespunzătoare schemei de management al incidentelor
    - 12 furnizori (38,7%) declară că au implementate proceduri privind unele dintre procesele acoperite;
    - Marea majoritate a furnizorilor care au proceduri tratează în cadrul acestora procesele de detectare și răspuns;
    - În general, procedurile tratează cazurile incidentelor frecvente și doar 50% dintre furnizorii ce dețin proceduri, tratează și incidentele predictibile, potențiale, excepționale, cunoscute sau necunoscute.

5. Vulnerabilități

Mai puțin de 50% din respondenți declară că tratează vulnerabilitățile în cadrul proceselor. Mai exact, în funcție de proces, avem următoarele statistici:

- Detectare și raportare - 14 furnizori (54%) tratează vulnerabilitățile în cadrul procesului;
- Evaluare - 12 furnizori (38,7%) tratează vulnerabilitățile în cadrul procesului;
- Răspuns - 12 furnizori (38,7%) tratează vulnerabilitățile în cadrul procesului;
- Colectare - 8 furnizori (25,8%) tratează vulnerabilitățile în cadrul procesului;
- 3 furnizori (9,7%) declară că tratează vulnerabilitățile și în cadrul procedurilor;
- 7 furnizori (22,6%) evaluează periodic vulnerabilitățile.

6. Incidente cibernetice

- 28 de furnizori (90,3%) declară că tratează incidentele cibernetice predominant din punctul de vedere al detectării și răspunsului la acestea;
- Doar 14 furnizori (45%) din cei ce tratează incidentele cibernetice dețin și o politică în acest sens;
- 19 furnizori (61%) dețin un sistem de detectare a incidentelor cibernetice; dintre aceștia, 10 furnizori dețin un sistem dedicat detectării incidentelor cibernetice;
- 21 de furnizori (67,7%) au menționat că echipa de răspuns la incidente se ocupă și de incidentele cibernetice și doar 7 furnizori (22,6%) au echipă dedicată;
- 7 furnizori (22,6%) documentează incidentele cibernetice în cadrul procedurilor;
- 6 furnizori (19%) mențin o evidență a incidentelor cibernetice înregistrate;
- 9,7% dintre furnizori nu tratează astfel de incidente.

7. Evaluarea schemei de management al incidentelor și analiza incidentelor

Deși 71 % dintre furnizorii chestionați declară că analizează periodic informațiile despre incidente pentru a identifica tendințe și domeniile ce necesită atenție specială, pentru a identifica măsurile ce pot fi luate pentru prevenirea unor incidente similare și pentru a determina și corecta deficiențele proceselor și procedurilor de management al incidentelor, doar 26% dintre furnizori întocmesc rapoarte anuale interne privind incidentele înregistrate. Nici unul dintre furnizori nu tratează în rapoarte și costurile implicate.

Așadar, se poate spune că în rândul furnizorilor se manifestă un interes scăzut în ceea ce privește documentarea analizei incidentelor, deși astfel de rapoarte pot oferi o imagine de ansamblu în ceea ce privește nivelul global al securității rețelelor și serviciilor de comunicații electronice în cadrul organizației, pot sprijini procesul de management al incidentelor și pot reprezenta un punct de plecare în implementarea unor noi măsuri de securitate.

Conform informațiilor primite privind analiza incidentelor, cel mai frecvent afectate categorii de resurse sunt cablurile (terestre, aeriene sau subterane), echipamentele auxiliare (de alimentare/de backup cu energie electrică, sisteme de răcire etc.) și routere și switch-uri IP.

În ceea ce privește măsurarea periodică a eficacității proceselor și procedurilor de management al incidentelor, doar 29% dintre furnizori au raportat că realizează această măsurare și nici unul dintre furnizori nu măsoară eficacitatea proceselor și procedurilor de management al incidentelor prin realizarea unor audituri interne SMSI sau prin analize SMSI.

8. Sisteme de detectare a incidentelor

Există sisteme, platforme și aplicații specifice dedicate:

- monitorizării rețelei și serviciilor de comunicații electronice - 24 de furnizori (77,4%).
- 48% dintre furnizorii respondenți declară că au stabilit parametri și praguri predefinite la atingerea cărora sistemul/sistemele de monitorizare generează alerte, notificări și rapoarte.
- monitorizării rețelei interne - 19 furnizori (61%). Răspunsurile au indicat faptul că nu au existat cazuri în care afectarea/compromiterea rețelei interne să conducă la afectarea furnizării rețelelor și serviciilor de comunicații electronice.
- monitorizării accesului neautorizat - 24 de furnizori (77,4%). Se poate observa din răspunsurile furnizorilor că cele mai utilizate sisteme de detectare a incidentelor cauzate de accesul neautorizat sunt sistemele de supraveghere, precum camere de supraveghere, supraveghere pe bază de senzori etc.
- monitorizării mediului – 10 furnizori (32,3%).

9. Proceduri și planuri de comunicare a incidentelor

16 furnizori (51,6%) au un proces de raportare a incidentelor către ANCOM, însă doar un furnizor deține proceduri specifice în care este detaliat acest proces și 4 furnizori țin o evidență a incidentelor raportate către ANCOM.
Există planuri de comunicare către:

- furnizori de rețele și servicii de comunicații electronice – 16 furnizori (51,6%),
- utilizatori – 11 furnizori (35,5%),
- parteneri de afaceri – 8 furnizori (26%),
- mass-media – 3 furnizori (10%).

Răspunsurile la Chestionarul privind implementarea măsurilor de securitate în domeniul managementului incidentelor au scos în evidență faptul că în rândul furnizorilor chestionați există o preocupare în ceea ce privește managementul incidentelor preponderent din punctul de vedere al proceselor de detectare și răspuns la incidente. O preocupare ceva mai scăzută există din punctul de vedere al politicii privind managementul incidentelor și al procedurilor documentate în care să fie tratate procesele.

Răspunsurile au scos în evidență un interes scăzut în ceea ce privește măsurarea și monitorizarea costurilor implicate în acțiunile de răspuns și/sau prevenire a unor incidente similare. Deși 8 furnizori au raportat că există mecanisme pentru a determina, măsura și monitoriza costurile implicate în acțiunile de răspuns și/sau prevenire a unor incidente similare, conform răspunsurilor, doar 2 furnizori țin evidența acestor informații în cadrul centralizatorului.

VI. ANEXĂ - Lista furnizorilor către care s-a transmis chestionarul

Nr.	Furnizor
1.	AKTA TELECOM S.A. (FOSTA ALT VAL NEW DIGITAL S.R.L.)
2.	AMBRA S.R.L.
3.	BANAT TELECOM SATELIT S.R.L. (FOSTA BĂLEANU SERVCOM S.R.L.)
4.	CABEL TV SISTEM S.R.L.
5.	CANAL S S.R.L.
6.	DIGI COMMUNICATION S.R.L.
7.	DIGITAL CATV S.R.L.
8.	ELECTROSIM S.R.L.
9.	ENIASAN S.R.L.
10.	EXPERTNET S.R.L.
11.	FAVORIT S.R.L.
12.	FOCUS SAT ROMANIA S.R.L.
13.	GLIGA COMIMPEX S.R.L.
14.	INES GROUP S.R.L.
15.	INTERSAT S.R.L.
16.	LIDAS PROD S.R.L.
17.	LYCAMOBILE S.R.L.
18.	MAGNAVOX COM FILIALA CRAIOVA S.R.L.
19.	MAGNOAVOX COM
20.	MEDIA SUD S.R.L.
21.	MILLENNIUM IT S.R.L.
22.	MULTIMEDIA NETWORK S.R.L.
23.	N & B TV SAT S.R.L.
24.	NORBERT COMUNICATION-IT S.R.L.
25.	NOVA SAT S.R.L.
26.	PRODCOMSERV VESZI S.R.L.
27.	TANGENT ELECTRO TRADE S.R.L.
28.	TELESAT S.R.L.
29.	TELESON S.R.L.
30.	TV ADLER-TRADING S.R.L.
31.	TV SAT 2002 S.R.L.