ANCOM
Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii

RAPORT
privind implementarea măsurilor de securitate în domeniul managementului incidentelor

martie 2015

CUPRINS

Introducere **2**

I. Procese şi proceduri privind managementul incidentelor **3**

1. Politica de management al incidentelor **3**

2. Compartimentul de tratare a incidentelor **5**

3. Schema de management al incidentelor **7**

3.1 PROCESE CORESPUNZĂTOARE SCHEMEI DE MANAGEMENT AL INCIDENTELOR 7
3.1.1 Detectare şi raportare 8
3.1.2 Evaluare/triere şi decizie 8
3.1.3 Răspuns 10
3.1.4 Escaladare 12
3.1.5 Colectarea informaţiilor despre incidente şi păstrarea evidenţei acestora 13
3.2 PROCEDURI CORESPUNZĂTOARE SCHEMEI DE MANAGEMENT AL INCIDENTELOR 14

4. Evaluarea schemei de management al incidentelor şi îmbunătăţiri **15**

4.1 ANALIZA SITUAŢIEI INCIDENTELOR ŞI ORGANIZAREA UNOR ÎNTÂLNIRI 16
4.2 DEPRINDEREA UNOR LECŢII ÎN URMA INCIDENTELOR ŞI ÎMBUNĂTĂŢIRI ASUPRA MĂSURILOR DE SECURITATE 17

II. Sistem de detectare a incidentelor **20**

1. Tipuri de detectare **21**

2. Monitorizarea funcţionării reţelelor şi serviciilor de comunicaţii electronice **22**

2.1. NECESITATEA MONITORIZĂRII/RESURSE MONITORIZATE 22
2.2 PRIMIREA SESIZĂRILOR/INDICIILOR/NOTIFICĂRILOR DESPRE INCIDENTE DIN PARTEA UNOR PERSOANE 22
2.3. PRIMIREA SESIZĂRILOR/INDICIILOR/NOTIFICĂRILOR DESPRE INCIDENTE DE LA ECHIPAMENTE/SISTEME 23
2.3.1 Monitorizarea reţelei interne/sistemelor informatice 23
2.3.2 Monitorizarea elementelor reţelei de comunicaţii electronice 24
2.3.3 Monitorizarea locaţiilor 25

3. Evaluarea şi actualizarea sistemului de detectare **27**

III. Proceduri şi planuri de comunicare a incidentelor **27**

1. Proceduri de raportare a incidentelor către ANCOM, precum şi către alte autorităţi responsabile **28**

2. Planuri de comunicare către alte părţi privind incidentele **28**

3. Modalităţi/instrumente de comunicare **29**

4. Evaluarea şi actualizarea planurilor şi procedurilor de comunicare/raportare a incidentelor **30**

IV. Alte informaţii **30**

V. Concluzii **33**

VI. Anexă **35**

Introducere

În vederea asigurării unor comunicaţii fiabile şi sigure prin intermediul reţelelor publice de comunicaţii electronice, potrivit dispoziţiilor art. 46 din Ordonanţa de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice aprobată, cu modificări şi completări, prin Legea nr. 140/2012, cu modificările şi completările ulterioare, furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului trebuie să adopte şi să implementeze toate măsurile adecvate, de ordin tehnic şi organizatoric, în vederea administrării riscurilor la adresa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice.

În acest sens, art. 3 din 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[1] prevede următoarele:

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

(2) Furnizorii de reţele publice de comunicaţii electronice au obligaţia de a lua toate măsurile de securitate necesare pentru a administra riscurile la adresa integrităţii reţelelor şi serviciilor de comunicaţii electronice, în scopul garantării integrităţii reţelelor şi al asigurării continuităţii furnizării serviciilor prin intermediul acestor reţele şi, acolo unde este cazul, de a colabora cu alţi furnizori pentru implementarea acestor măsuri.

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

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

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 securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice din perspectiva măsurilor de securitate implementate de furnizori în acest domeniu, conform prevederilor legale.

Pentru a evalua stadiul de implementare a măsurilor de securitate în domeniul managementului incidentelor, ANCOM a transmis către 16 furnizori[2] de reţele şi servicii de comunicaţii electronice un chestionar privind implementarea măsurilor de securitate în domeniul managementului incidentelor[3]. Furnizorii chestionaţi au fost cei cu mai mult de 100.000 de abonaţi, precum şi cei care deţin o reţea naţională de comunicaţii electronice.

În cadrul acestui chestionar, *managementul incidentelor* implică stabilirea/dezvoltarea/ implementarea unor planuri de acţiune, a unui set de procese şi proceduri consistente, repetabile,

---

[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 poate fi consultată aici: http://www.ancom.org.ro/formdata-1130-48-1703

[2] Lista furnizorilor către care s-a transmis chestionarul se regăseşte în anexa la prezentul raport.

[3] 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 găseşte aici:
http://www.ancom.org.ro/uploads/links_files/Adresa_masuri_de_securitate_in_domeniul_managementului_incidentelor.pdf

măsurabile şi utilizarea unor mijloace adecvate de natură administrativă, managerială, tehnică sau juridică în vederea detectării, analizei şi răspunsului la incidentele ce au loc în cadrul organizaţiei şi care afectează sau pot afecta furnizarea reţelelor şi serviciilor de comunicaţii electronice. Totodată, în cadrul prezentului chestionar se aplică definiţiile menţionate în Decizia preşedintelui Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii nr.512/2013.

De asemenea, furnizorilor li s-a solicitat să ataşeze/anexeze chestionarului documente relevante (în limba română sau engleză) care să susţină răspunsurile oferite.

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

I. Procese şi proceduri privind managementul incidentelor

Conform Deciziei nr.512/2013, furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia să stabilească procese şi proceduri pentru managementul incidentelor care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice (care să vizeze raportarea internă, evaluarea, răspunsul la incidente şi escaladarea acestuia), inclusiv prin definirea rolurilor şi responsabilităţilor.

1. Politica de management al incidentelor

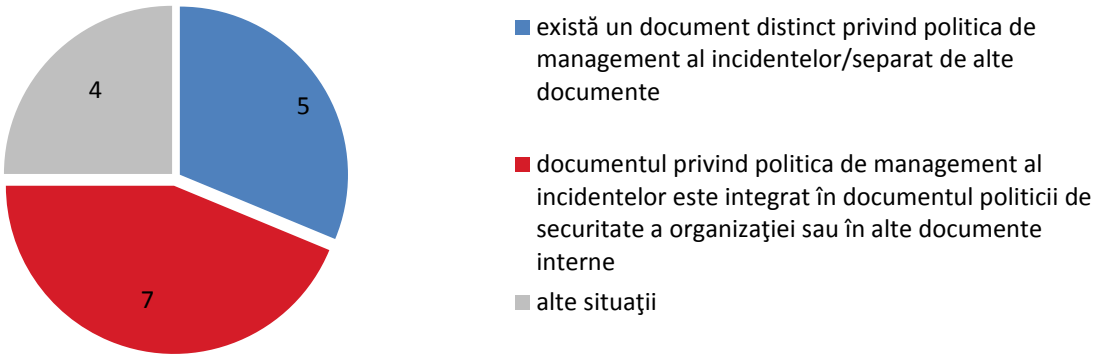
Politica de management al incidentelor reprezintă acel document care trasează o direcţie clară a organizaţiei în domeniul managementului incidentelor şi la baza căruia stau procesele şi procedurile aferente acestui domeniu, precum şi resursele/mecanismele/capabilităţile (tehnice, operaţionale etc.) ce susţin aceste procese şi proceduri.

Aceasta poate să abordeze/să cuprindă aspecte precum:

- importanţa procesului de management al incidentelor pentru organizaţie şi angajamentul conducerii organizaţiei în sprijinirea managementului incidentelor;
- scopul, obiectivele şi domeniul de aplicare a politicii (cui se aplică, în ce condiţii etc.);
- definirea unor termeni specifici, încadrabili în contextul managementului incidentelor;
- descrierea proceselor de detectare, raportare şi colectare a informaţiilor despre evenimentele ce afectează/pot afecta securitatea, inclusiv prin corelarea acestor procese cu tipuri de incidente frecvente/predictibile;
- modul de analiză, evaluare (incluzând triere, prioritizare) a incidentelor;
- activităţile ce trebuie întreprinse în vederea remedierii incidentelor/răspunsului la acestea;
- înregistrarea tuturor activităţilor desfăşurate în vederea unor analize ulterioare şi păstrarea sigură a evidenţei electronice privind incidentele înregistrate;
- activităţi post-incident incluzând evaluarea incidentelor şi îmbunătăţirea proceselor şi procedurilor din cadrul schemei de management al incidentelor;
- aspecte referitoare la raportarea şi tratarea vulnerabilităţilor;
- aspecte privind proceduri operaţionale, formulare de raportare a incidentelor etc.;
- descrierea personalului care se ocupă de managementul incidentelor/echipei de răspuns la incidente, inclusiv prin descrierea rolurilor şi responsabilităţilor aferente;
- informaţii privind mecanismele/resursele/capabilităţile ce asigură suportul tehnic, operaţional etc.;
- aspecte privind diseminarea informaţiilor despre incidente unor părţi externe;
- actele normative ce trebuie respectate şi alte aspecte legale ce trebuie luate în considerare.

Graficul următor ilustrează situaţia furnizorilor chestionaţi în ceea ce priveşte existenţa unei politici de management al incidentelor/unui document privind politica de management al incidentelor în cadrul propriilor organizaţii.

Fig.1 Politica de management al incidentelor



Astfel, pentru 5 furnizori există un document distinct privind politica de management al incidentelor/separat de alte documente, documentul privind politica de management al incidentelor este integrat în documentul politicii de securitate a organizaţiei sau în alte documente interne pentru alţi 7, restul furnizorilor chestionaţi (4) având un set de documente care reglementează modul de identificare, tratare şi raportare a incidentelor, inclusiv responsabilităţile asociate acestor activităţi.

Conform răspunsurilor primite, această politică de management al incidentelor/documentul privind politica de management al incidentelor vizează şi incidentele cibernetice[4] pentru 10 dintre furnizorii chestionaţi, 5 furnizori deţin o politică distinctă (un alt document de politică) privind aceste incidente, iar un furnizor a afirmat că aspectele referitoare la incidentele cibernetice nu se aplică în cazul său datorită specificului reţelei de comunicaţii electronice.

Furnizorilor li s-a solicitat să descrie politica de management al incidentelor, dar şi politica/planul de răspuns la incidente, punctând elementele conţinute de acestea. Descrierile au scos în evidenţă faptul că în rândul majorităţii furnizorilor nu există o distincţie clară între documentul politicii de management al incidentelor, politica/planul de răspuns la incidente şi procedurile documentate asociate acestui domeniu. Astfel, în rândul furnizorilor chestionaţi există diverse abordări în ceea ce priveşte documentaţia aferentă managementului incidentelor şi mai multe tipuri de documente/modalităţi de prezentare a proceselor, rolurilor şi responsabilităţilor asociate managementului incidentelor. Abordările şi/sau modalităţile în care sunt prezentate aspectele referitoare la managementul incidentelor variază de la un furnizor la altul în funcţie de normele interne ale organizaţiei.

Conform răspunsurilor la chestionar, în cadrul documentelor interne (politici, proceduri, metodologii etc.) privind managementul incidentelor sunt stabilite principiile, etapele şi acţiunile aferente identificării, evaluării şi rezolvării incidentelor, inclusiv escaladării acestora şi sunt descrise rolurile persoanelor implicate în activităţile aferente. Aceste documente constau de obicei în descrierea proceselor/etapelor/activităţilor asociate gestionării diverselor tipuri de evenimente/incidente în funcţie de impactul lor, resurse implicate, persoane/echipe responsabile de tratare etc..

De regulă, politica, procesele şi procedurile de management al incidentelor sunt comunicate/vizibile întregului personal al organizaţiei şi se adresează cu precădere personalului cu

[4] 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.

atribuţii de specialitate în domeniu (personalului tehnic implicat/entităţilor participante în procesele de detectare, rezolvare, închidere a incidentelor). O parte dintre furnizorii chestionaţi au menţionat şi alte părţi cărora li se adresează aceste documente, de exemplu colaboratorilor şi reprezentanţilor partenerilor contractuali care au acces autorizat pentru desfăşurarea de activităţi specifice.

2. Compartimentul de tratare a incidentelor

În ceea ce priveşte existenţa unui compartiment dedicat activităţilor de tratare/management al incidentelor, răspunsurile la întrebarea dedicată au scos în evidenţă următoarele aspecte:

- 8 furnizori au precizat că există un compartiment/departament dedicat activităţilor de tratare/management al incidentelor, cu echipă de răspuns la incidente în cadrul propriilor organizaţii; dintre aceştia 8, un furnizor a menţionat că echipa este în curs de formare, existând la acest moment mai multe echipe separate, dedicate anumitor tipuri de incidente, iar altul a ţinut să precizeze că pe lângă acest compartiment dedicat, există şi alte compartimente/persoane cu responsabilităţi în domeniu, cu roluri specifice în procesul transversal de gestionare a incidentelor (compartimente cu responsabilităţi în ceea ce priveşte relaţiile cu clienţii, supervizarea reţelei de comunicaţii electronice, monitorizarea şi mentenanţa serviciilor, operare în teren etc.); conform răspunsurilor la o altă întrebare din chestionar, pentru 3 dintre aceşti 8 furnizori, activităţile de monitorizare a reţelei/serviciilor/echipamentelor/aplicaţiilor sunt realizate de personalul organizaţiei şi de părţi subcontractate;
- 5 furnizori au afirmat că nu există un astfel de compartiment, dar sunt desemnate persoane care să se ocupe de managementul/tratarea incidentelor;
- 3 furnizori au un contract de prestări servicii în acest sens/aceste servicii sunt externalizate, dar în cazul lor există şi structuri interne dedicate activităţilor de tratare a incidentelor.

Printre tipurile de incidente menţionate de furnizori şi care intră în aria de competenţă/activitate a compartimentului de tratare a incidentelor/echipei de răspuns la incidente se află acele evenimente care pot afecta resursele, procesele sau obiectivele organizaţiei, incidente ce afectează funcţionarea reţelelor şi serviciilor de comunicaţii electronice, incidente de securitate cibernetică.

Dintre tipurile de incidente care afectează funcţionarea reţelelor şi serviciilor de comunicaţii electronice, au fost precizate:

- incidente privind disponibilitatea reţelei;
- incidente privind frauda pentru servicii de voce;
- lipsa energiei electrice;
- distrugerea fibrei optice;
- incendii, explozii sau inundaţii;
- furt de echipamente;
- dezactivarea sistemelor de control de securitate;
- erori ale aplicaţiilor;
- probleme de *peering*, pierderi de pachete etc..

Incidentele de securitate fizică (acces neautorizat în incinta organizaţiei etc.) au fost menţionate frecvent în rândul furnizorilor chestionaţi. De asemenea, au fost precizate şi tipuri de incidente cibernetice care pot afecta funcţionarea reţelelor şi serviciilor de comunicaţii electronice, precum:

- încercări repetate de acces sau acces/utilizare neautorizat/ă a sistemelor informatice ale organizaţiei;
- pierderea fizică, furtul, coruperea sau distrugerea neautorizată a resurselor informatice;

- infiltrarea de viruşi, viermi, troieni sau alte software-uri maliţioase în sistemele informatice;

- căderi ale sistemului informatic sau ale serviciilor acestuia;

- divulgarea neautorizată, modificarea sau utilizarea greşită sau necorespunzătoare a resurselor informatice;

- compromiterea conturilor utilizatorilor sau a parolelor;

- sisteme care lucrează lent, sunt instabile sau inaccesibile;

- atacuri *DDoS*[5].

Furnizorii au descris succint principalele activităţi ale compartimentului de tratare a incidentelor/echipei de răspuns la incidente. După caz, unii furnizori au precizat activităţi desfăşurate în cadrul *NOC-ului*[6], alţii au punctat activităţile unor echipe dedicate diverselor procese asociate managementului incidentelor, inclusiv activităţi ale personalului implicat în servicii de relaţii cu clienţii. Conform descrierilor, principalele activităţi includ:

- monitorizarea elementelor de reţea;

- analiza alarmelor provenite de la echipamentele de monitorizare a serviciilor;

- preluarea, analiza şi soluţionarea sesizărilor primite de la abonaţi;

- înregistrarea incidentelor în sistemul de *ticketing* al organizaţiei;

- încadrarea incidentelor în funcţie de clasificările/nivelele de severitate agreate;

- stabilirea impactului incidentelor;

- notificarea managementului în cazul incidentelor cu prioritate ridicată;

- escaladarea către nivele superioare de operare;

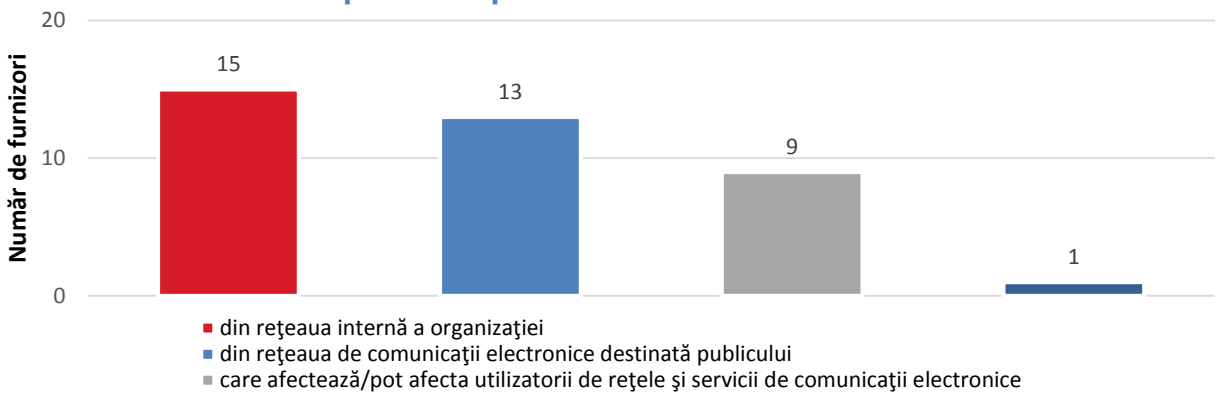
- tratarea incidentelor conform bunelor practici din domeniu şi conform experienţei tehnicienilor şi inginerilor din echipele de suport tehnic;

- urmărirea rezolvării şi închiderea incidentelor.

Pentru 7 dintre furnizori, compartimentul de tratare a incidentelor/echipa de răspuns la incidente are roluri şi responsabilităţi privind tratarea/managementul incidentelor cibernetice, 6 furnizori au o echipă dedicată tratării/managementului incidentelor cibernetice, iar pentru alţi 3 respondenţi sunt valabile alte situaţii, precum: tratarea incidentelor cibernetice este realizată de o echipă mixtă, echipa de răspuns la incidente are la acest moment şi rol în tratarea şi managementul incidentelor cibernetice, urmând ca în viitor să existe o echipă separată/dedicată.

Figura 2 ilustrează tipul incidentelor cibernetice tratate de compartimentul de tratare a incidentelor/echipa de răspuns la incidente sau de echipa dedicată.

Fig.2 Compartimentul de tratare a incidentelor/echipa de răspuns la incidente sau după caz echipa dedicată tratează incidentele cibernetice:



[5] Distributed Denial of Service
[6] Network Operations Center

Pentru 8 dintre furnizori, compartimentul de tratare a incidentelor/echipa de răspuns la incidente sau după caz, echipa dedicată, tratează incidentele cibernetice din reţeaua internă a organizaţiei, din reţeaua de comunicaţii electronice destinată publicului, dar şi acele incidente care afectează/pot afecta utilizatorii de reţele şi servicii de comunicaţii electronice. Pentru alţi 5 furnizori sunt tratate doar incidentele cibernetice din reţeaua internă a organizaţiei şi cele din reţeaua de comunicaţii electronice destinată publicului. Un furnizor tratează numai incidentele cibernetice din reţeaua internă a organizaţiei şi pe cele care afectează/pot afecta utilizatorii de reţele şi servicii de comunicaţii electronice, altul doar pe cele din reţeaua internă a organizaţiei.

3. Schema de management al incidentelor[7]

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

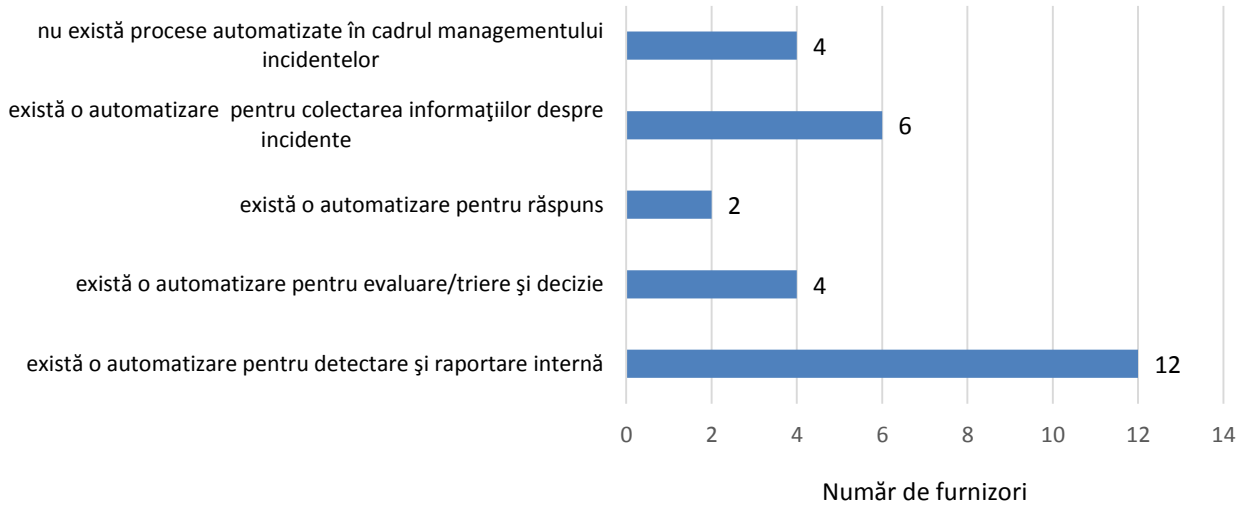
Răspunsurile la chestionar au indicat că furnizorii deţin o schemă de management al incidentelor. În general, schema de management al incidentelor tratează etapele gestionării incidentelor, oferind îndrumări privind modul de detectare, analiză, clasificare, prioritizare, răspuns la evenimente/incidente/vulnerabilităţi.

Schema de management al incidentelor vizează şi incidentele cibernetice pentru 9 furnizori, pentru alţi 5 furnizori există procese şi proceduri specifice acestui tip de incidente, 1 furnizor nu a răspuns la întrebarea dedicată, iar pentru altul contextul este diferit având în vedere specificul reţelei de comunicaţii electronice.

3.1 Procese corespunzătoare schemei de management al incidentelor

Figura 3 oferă o imagine asupra automatizării proceselor privind managementul incidentelor în rândul furnizorilor chestionaţi.

Fig.3 Automatizarea proceselor de management al incidentelor



[7] **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.

Procesul de detectare şi raportare internă este automatizat pentru 12 dintre furnizorii chestionaţi. Automatizarea pentru acest proces se referă de regulă la existenţa unor sisteme de monitorizare a elementelor reţelei de comunicaţii electronice (monitorizarea alarmelor generate de elementele de reţea). Celelalte procese de management al incidentelor (evaluare/triere şi decizie, răspuns, colectare a informaţiilor despre incidente) sunt automatizate în rândul unui număr restrâns de furnizori. Pentru 4 furnizori nu există procese automatizate în cadrul managementului incidentelor.

3.1.1 Detectare şi raportare

Descrierea subproceselor/activităţilor uzuale asociate detectării şi raportării evenimentelor/incidentelor/vulnerabilităţilor în rândul furnizorilor chestionaţi a scos în evidenţă practici precum:

- detectarea incidentelor prin sistemele de monitorizare şi raportarea către compartimentele/echipele responsabile;
- monitorizarea alarmelor din reţea;
- monitorizarea traficului şi a logurilor;
- raportarea/notificarea evenimentelor de către angajaţi sau terţi;
- identificarea incidentelor prin accesul direct pe echipamentele de reţea;
- urmărirea reţelei prin intermediul unor sisteme software dedicate;
- primirea în mod automat a unor informaţii provenite de la senzori, roboţi.

10 furnizori iau în considerare vulnerabilităţile în cadrul procesului de detectare şi raportare.

Capitolul II. Sistem de detectare a incidentelor oferă mai multe informaţii cu privire la procesul de detectare a incidentelor, la mijloacele/instrumentele utilizate în acest proces.

3.1.2 Evaluare/triere şi decizie

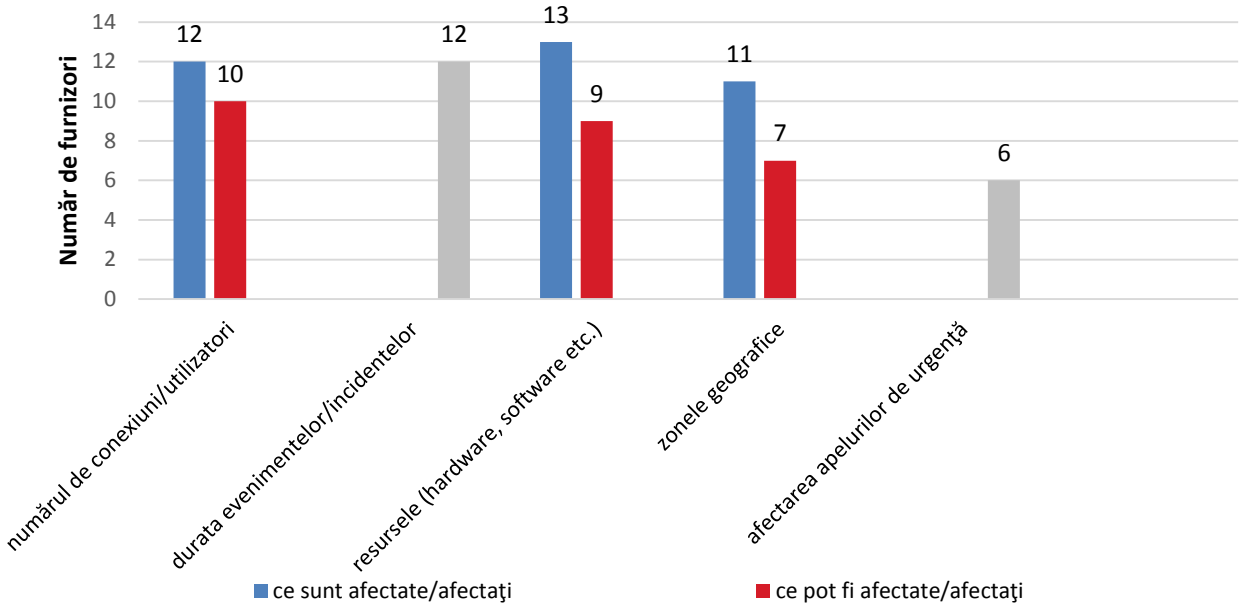
Procesul de evaluare/triere şi decizie se referă la acţiunile întreprinse după detectarea evenimentelor/incidentelor în vederea asigurării unui răspuns rapid, eficient şi organizat. Determinarea impactului incidentului asupra furnizării reţelelor şi serviciilor de comunicaţii electronice, asupra proceselor afacerii pe baza încadrării acestuia în anumite categorii (de exemplu incidente minore, majore, critice) conduce, de regulă, la decizii asupra soluţiilor de remediere, modului de prioritizare a acţiunilor de răspuns, asupra nivelelor necesare de escaladare a răspunsului la incident.

Descrierea subproceselor uzuale asociate evaluării/trierii evenimentelor/incidentelor şi deciziei asupra modului de răspuns/tratare a incidentelor a evidenţiat principalele activităţi ale furnizorilor chestionaţi în această privinţă:

- analiza informaţiilor 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.

Aşa cum se observă din graficul de mai jos, impactul evenimentelor/incidentelor asupra furnizării reţelelor şi serviciilor de comunicaţii electronice se determină de regulă ţinând cont de numărul de conexiuni/utilizatori ce sunt afectaţi, durata evenimentelor/incidentelor, resursele şi zonele geografice ce sunt afectate.

Fig.4 Determinarea impactului evenimentului/incidentului asupra furnizării reţelelor şi serviciilor de comunicaţii electronice ţine cont de:



Pentru estimarea numărului de conexiuni/utilizatori afectate/afectaţi de un incident, furnizorii au indicat metode diferite, în funcţie de tipul serviciilor de comunicaţii electronice furnizate (fixe sau mobile). Pentru estimarea numărului de conexiuni mobile afectate de un incident, unii furnizori au menţionat metoda impusă de ANCOM prin Decizia nr.512/2013 (compararea traficului afectat la momentul incidentului cu traficul înregistrat în acelaşi interval de timp, în perioada anterioară). Pentru estimarea numărului de conexiuni fixe afectate de un incident, metodele descrise de furnizorii chestionaţi implică:

- utilizarea unor instrumente de monitorizare prin care se identifică clienţii impactaţi şi corelarea cu răspândirea geografică a clienţilor care apelează serviciile de *call center*;

- existenţa unei legături software între sistemul de facturare şi cel de monitorizare, astfel încât la fiecare moment se cunoaşte numărul de clienţi deserviţi de fiecare element de reţea;

- identificarea zonei geografice afectate de un incident prin intermediul sistemului de monitorizare a reţelei şi ulterior identificarea numărului de clienţi afectaţi;

- calculul unor medii de clienţi afectaţi în funcţie de categoria de reţea, aria geografică şi tehnologia afectate.

Pentru estimarea impactului incidentelor cibernetice, furnizorii folosesc metode similare celor utilizate pentru estimarea impactului incidentelor de reţea.

Toţi furnizorii chestionaţi au un proces de clasificare/triere a evenimentelor/incidentelor petrecute în cadrul organizaţiei.

Clasificarea evenimentelor/incidentelor este utilă pentru determinarea nivelului de severitate a acestora şi implicit pentru stabilirea acţiunilor de remediere necesare. Cei mai mulţi furnizori au indicat numărul utilizatorilor afectaţi ca fiind criteriul după care se realizează clasificarea evenimentelor/incidentelor. Abordarea în privinţa clasificării evenimentelor/incidentelor este simplificată (de exemplu cu 3 nivele) pentru unii furnizori sau amplă (de exemplu cu 5 nivele) pentru alţii.

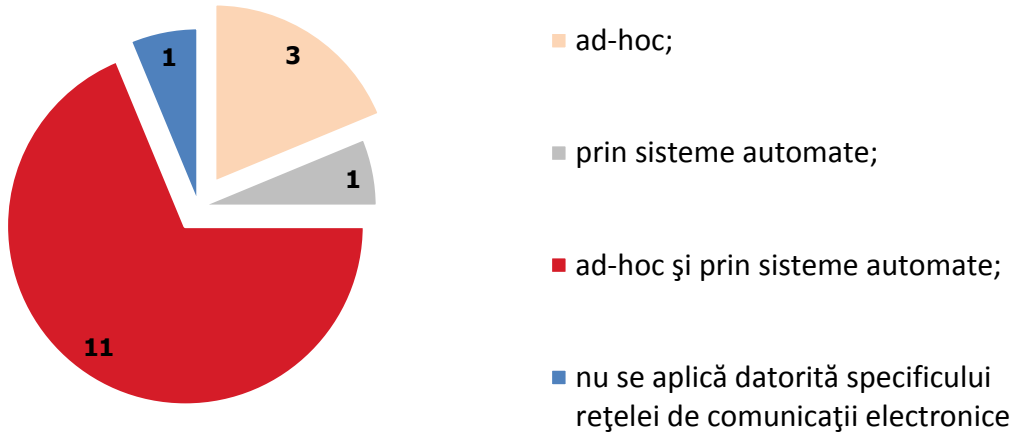
9 furnizori (din cei 16 chestionaţi) deţin o situaţie a evenimentelor/incidentelor înregistrate pe parcursul anului 2014 pentru fiecare categorie corespunzatoare clasificărilor precizate.

Pentru cei mai mulţi dintre furnizorii chestionaţi, prioritizarea evenimentelor/incidentelor în vederea răspunsului atunci când se înregistrează mai multe evenimente simultan se bazează pe nivelul lor de severitate/criticitate, realizându-se în funcţie de impactul asupra utilizatorilor afectaţi/serviciilor afectate.

Pentru a prioritiza eforturile echipei de răspuns, poate fi necesară corelarea evenimentelor/incidentelor (verificarea dependenţei de alte incidente). Corelarea evenimentelor este utilă de exemplu în cazul evenimentelor provenite de la mai multe surse, pentru găsirea cauzei comune a unor incidente similare, în cazul incidentelor repetitive, al căror impact individual nu este unul puternic, însă prin repetarea acestora impactul cumulat se accentuează, atingând amploarea unui incident major.

Furnizorii corelează evenimentele/incidentele trecute sau în curs de desfăşurare. 12 furnizori corelează evenimentele/incidentele prin sisteme automate, dar şi ad-hoc, iar 3 furnizori folosesc numai metode ad-hoc de corelare (figura 5).

Fig.5 Cum corelaţi evenimentele?



Corelarea evenimentelor se realizează:

- prin utilizarea unor platforme de management, aplicaţii de *trouble ticketing;*
- prin observarea simultană a alarmelor provenite de la diverse sisteme de monitorizare;
- utilizând sistemele de monitorizare corelate cu sistemul de *call center*;
- la nivelul elementelor de agregare a traficului pentru unele servicii de comunicaţii electronice;
- prin utilizarea unor instrumente dedicate analizei logurilor de pe echipamente;
- pe baza informaţiilor primite de la sistemele de management centralizat şi de la dispeceratele regionale;
- ad-hoc de către personalul responsabil etc..

9 furnizori iau în considerare vulnerabilităţile în cadrul procesului de evaluare/triere şi decizie.

3.1.3 Răspuns

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

Pentru 10 furnizori procesul de răspuns la evenimente/incidente vizează şi incidentele cibernetice. În cazul majorităţii celorlalţi furnizori există un proces distinct de răspuns la astfel de incidente.

Estimarea perioadei de timp necesare restabilirii serviciilor de comunicaţii electronice afectate în parametrii normali de funcţionare se realizează în funcţie de factori precum: resursa afectată, informaţiile primite de la echipele din teren precum şi de la terţi, capacitatea echipei de răspuns, necesitatea deplasării în teren/accesul fizic pentru soluţionare/distanţa până la locaţie, condiţiile meteorologice, măsurile ce trebuie luate pentru remedierea incidentului, localizarea elementului afectat, clasificarea incidentului, tipul şi gravitatea evenimentului, rezultatul analizei ad-hoc pentru fiecare incident, evaluarea sistemelor/infrastructurii afectate, baremul intern impus pentru fiecare prioritate.

Toţi furnizorii chestionaţi dispun de posibilitatea răspunsului imediat la incidente. Totodată, aceştia dispun şi de posibilitatea răspunsului ulterior/pe termen lung la incidente.

Printre cel mai frecvent utilizate categorii de acţiuni de răspuns imediat la incidente au fost menţionate:

- organizarea activităţilor de răspuns/activităţi logistice (de exemplu organizarea echipelor de intervenţie din punct de vedere al resurselor umane, al echipamentelor de intervenţie, aspectelor referitoare la deplasare, dispecerizarea echipelor în teren pentru rezolvarea problemelor);

- utilizarea soluţiilor 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/soluţii (de exemplu înlocuirea unor echipamente defecte, refacerea traseului de cablu deteriorat sau alte intervenţii în cazul distrugerilor/furturilor de suport de comunicaţii, depanarea sistemelor informatice, reconfigurarea/reiniţializarea unor echipamente/sisteme software, reconfigurări de parametri, intervenţia manuală, relocarea fizică);

- cooperarea cu alte părţi - alţi furnizori de reţele şi servicii de comunicaţii electronice, furnizori de utilităţi, producători de echipamente etc. (de exemplu cooperarea cu furnizori de energie electrică, contactarea producătorilor de echipamente pentru escaladare).

Printre cel mai frecvent utilizate categorii de acţiuni de răspuns ulterior/pe termen lung la incidente au fost menţionate:

- acţiuni de remediere/restabilire completă a sistemelor/reţelelor/serviciilor;

- implementarea unor măsuri tehnice şi organizatorice pentru prevenirea altor incidente similare/actualizarea măsurilor tehnice existente (de exemplu achiziţionarea de echipamente pentru înlocuirea celor afectate, actualizarea proceselor, politicilor şi procedurilor operaţionale, implementarea unor soluţii de back-up, schimbarea tehnologiilor/soluţiilor tehnice, contractarea unor servicii, modificări în configuraţia reţelei pentru minimizarea impactului unui potenţial incident/redesign al soluţiei/platformei/cluster-ului de reţea, îmbunătăţirea mecanismelor de detectare a incidentelor, implementarea unor măsuri de securitate fizică, implementarea de noi platforme de servicii sau elemente de reţea, schimbarea vendorului de echipamente de reţea/platforme de servicii);

- analize post-incident şi verificarea/monitorizarea sistemelor/reţelelor/serviciilor (de exemplu analiză post-incident care conţine cauza incidentului, modul de soluţionare şi acţiuni post-incident pentru evitarea incidentelor de acelaşi tip, testarea preventivă a sistemelor neafectate, simulări de atacuri cibernetice, evaluarea riscurilor, urmărirea modului de funcţionare a sistemelor/echipamentelor implicate pe o anumită perioadă de timp, monitorizarea soluţiilor adoptate pentru răspunsul la incidente).

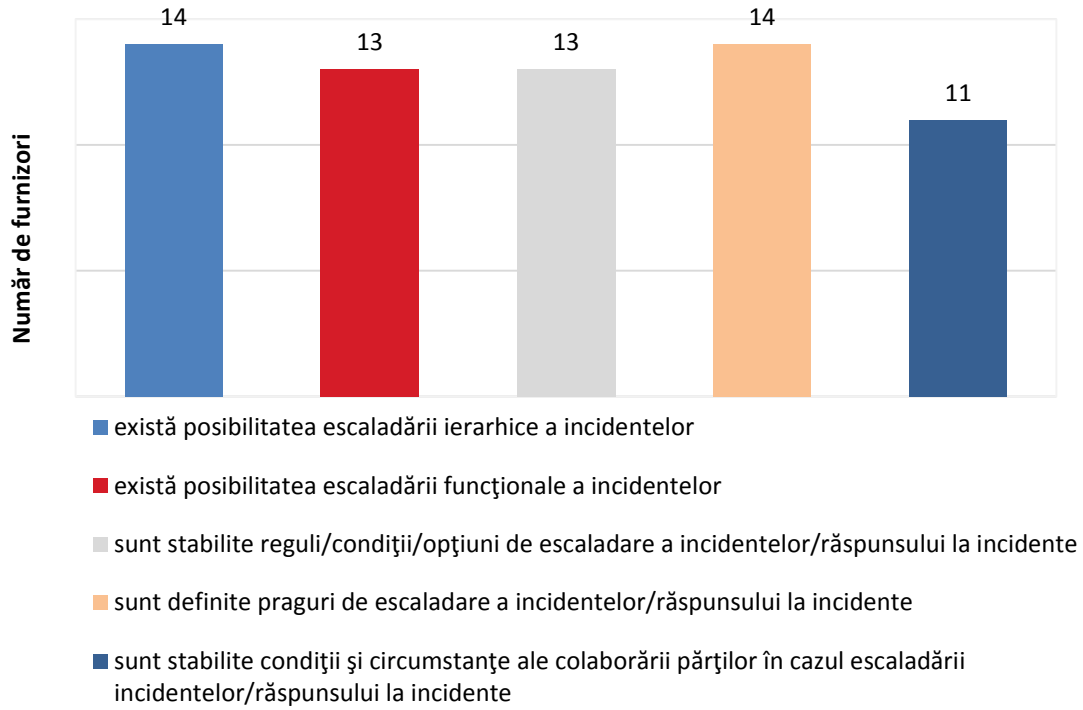
14 furnizori deţin un proces de răspuns în caz de urgenţă/criză în care sunt identificate opţiuni de tratare a unor incidente ce cauzează perturbări grave ale funcţionării reţelei sau serviciului de comunicaţii electronice.

9 furnizori iau în considerare vulnerabilităţile în cadrul procesului de răspuns.

3.1.4 Escaladare

Figura 6 prezintă procesul escaladării incidentelor/răspunsului la incidente în rândul furnizorilor chestionaţi.

Fig.6 Escaladarea incidentelor/răspunsului la incidente



Astfel, pentru majoritatea furnizorilor escaladarea incidentelor/răspunsului la incidente este un proces căruia i se acordă atenţie, existând atât posibilitatea escaladării ierarhice[8], cât şi posibilitatea escaladării funcţionale a incidentelor[9].

În rândul furnizorilor chestionaţi, necesitatea escaladării incidentelor/răspunsului la incidente depinde de intervalul de timp alocat remedierii incidentelor, de schimbarea priorităţii de rezolvare a incidentului. În unele cazuri, escaladarea are loc atunci când resursele solicitate echipei de intervenţie depăşesc resursele alocate sau competenţele atribuite. De regulă, furnizorii deţin nivele de escaladare în funcţie de normele interne. Astfel, escaladarea funcţională se realizează în funcţie de aria de expertiză a diverselor părţi implicate (de exemplu, există 4 nivele de escaladare funcţională: nivelul 1 – incidente ce pot fi tratate şi remediate de echipa care le-a detectat, nivelul 2 – incidente ce pot fi tratate de echipe de experţi, nivelul 3 – incidente ce pot fi tratate de echipe din teren, nivelul 4 - incidente ce pot fi tratate de furnizorii de echipamente). Escaladarea ierarhică se realizează la depăşirea unor praguri de timp prestabilite şi asociate severităţii incidentului, în funcţie de nivelul afectării *SLA*[10] etc. Pe de altă parte, escaladarea ierarhică este utilizată de unii furnizori în cazul incidentelor critice.

[8] Escaladarea ierarhică poate însemna escaladarea în luarea deciziilor privind modul de încadrare a evenimentelor în anumite categorii prestabilite, de prioritizare a activităţilor de răspuns pentru un anumit incident sau în ceea ce priveşte tipul acţiunilor de remediere/răspuns.
[9] Escaladarea funcţională poate însemna transferul unui incident/eveniment către o echipă tehnică cu un alt nivel de expertiză pentru a asista în răspunsul la incident.
[10] Service Level Agreement

3.1.5 Colectarea informaţiilor despre incidente şi păstrarea evidenţei acestora

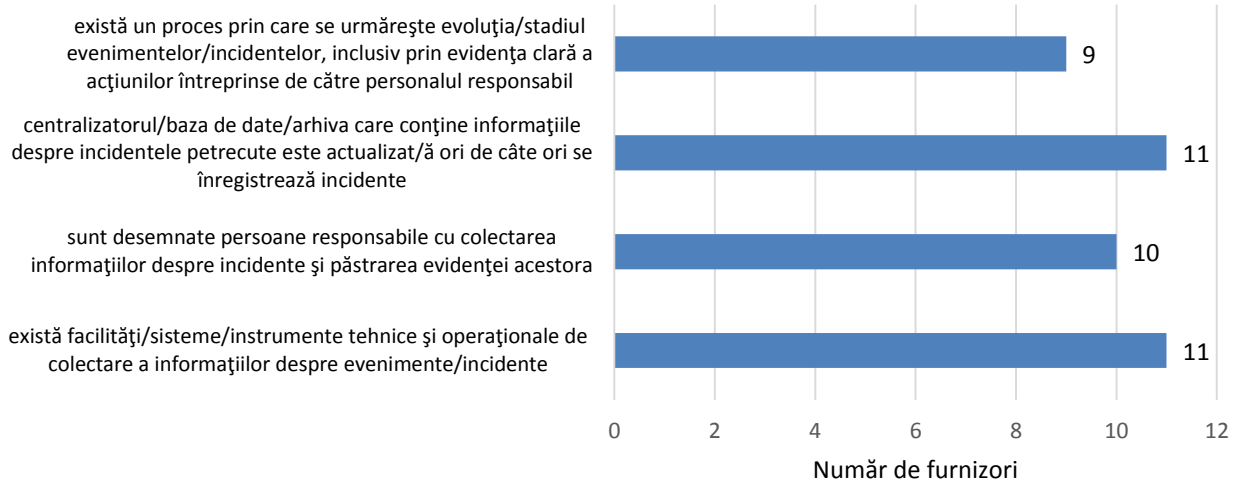
Toţi furnizorii chestionaţi au afirmat că au o evidenţă a incidentelor petrecute în cadrul propriilor organizaţii. Astfel, 13 furnizori păstrează evidenţa incidentelor pe suport electronic, 2 furnizori atât pe suport fizic, cât şi electronic şi 1 furnizor pe suport fizic.

Toţi furnizorii au o evidenţă/înregistrări privind incidentele petrecute în anul 2014.

12 furnizori dintre cei chestionaţi au o evidenţă a incidentelor cibernetice petrecute în cadrul organizaţiei.

Din graficul de mai jos reiese interesul acordat de furnizori pentru procesul de colectare a informaţiilor despre incidente şi păstrarea evidenţei acestora.

Fig.7 Colectarea informaţiilor despre incidente şi păstrarea evidenţei acestora

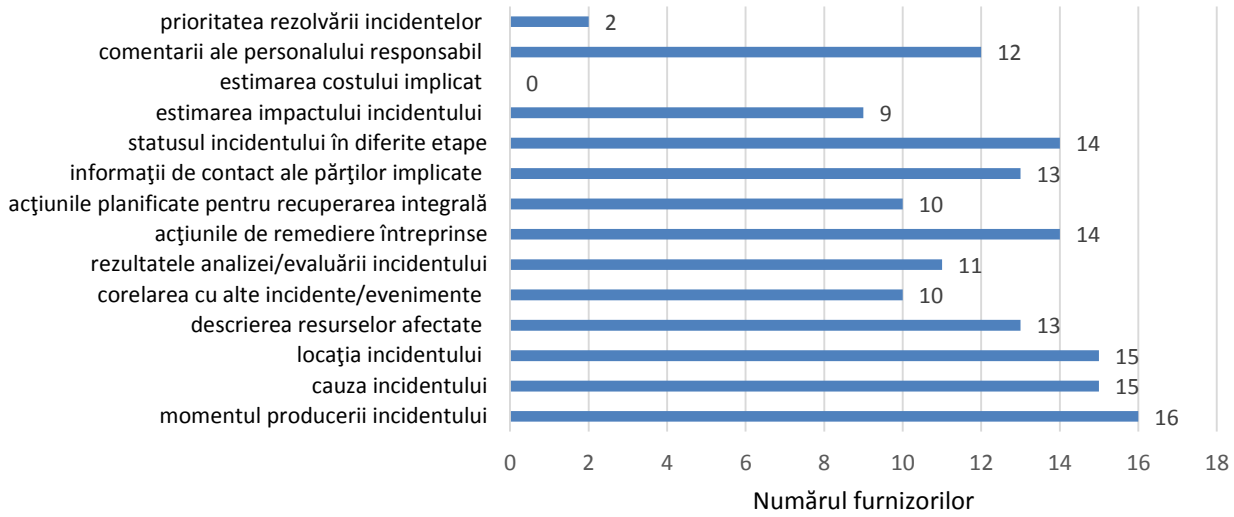


Vulnerabilităţile sunt luate în considerare în cadrul procesului de colectare a informaţiilor despre incidente şi păstrarea evidenţei acestora pentru 9 dintre cei chestionaţi.

Momentul producerii incidentului, cauza incidentului, locaţia incidentului (aria geografică afectată, dar şi identificarea locaţiei resurselor afectate) sunt câteva dintre informaţiile conţinute în baza de date/centralizatorul incidentelor pentru majoritatea furnizorilor (figura 8).

Alte informaţii stocate se referă la: descrierea resurselor afectate (echipamente etc.), corelarea cu alte incidente/evenimente asociate (dacă este cazul), rezultatele analizei/evaluării incidentului, respectiv deciziile luate în vederea remedierii sale, acţiunile întreprinse în vederea remedierii incidentului, acţiunile planificate pentru recuperarea integrală în urma incidentului şi pentru prevenirea altor incidente similare, informaţii de contact ale părţilor implicate – ale celui ce detectează/raportează incidentul şi ale celui/celor ce se ocupă de tratarea acestuia, statusul incidentului în diferite etape/momente de timp pe tot parcursul desfăşurării sale, estimarea impactului incidentului asupra proceselor afacerii, implicit asupra furnizării reţelelor şi serviciilor de comunicaţii electronice, comentarii ale personalului responsabil cu managementul incidentelor, prioritatea rezolvării incidentelor.

Fig.8 Informaţii conţinute în baza de date/centralizatorul incidentelor



Printre activităţile asociate procesului de colectare a informaţiilor despre incidente şi păstrarea evidenţei acestora se regăsesc:

- completarea unor formulare de raportare a incidentelor;
- centralizarea informaţiilor despre incidente;
- realizarea de rapoarte zilnice/lunare/săptămânale pentru incidentele din reţea;
- arhivarea informaţiilor despre incidente.

Unii furnizori colectează informaţii doar despre incidentele majore petrecute.

Pentru o parte dintre furnizori nu este stabilită o perioadă de păstrare a evidenţei incidentelor, alţii precizează perioade de minim 6 luni, 2 ani, 3 ani, 5 ani. Există şi categoria celor care afirmă că evidenţa incidentelor se păstrează pe perioadă nelimitată.

3.2 Proceduri corespunzătoare schemei de management al incidentelor

Procedurile documentate corespunzătoare managementului incidentelor vizează incidente ce afectează/pot afecta furnizarea reţelelor şi serviciilor de comunicaţii electronice pentru toţi furnizorii chestionaţi. Pentru 15 dintre aceştia, procedurile vizează şi evenimente ce afectează/pot afecta furnizarea reţelelor şi serviciilor de comunicaţii electronice, iar doar pentru 4 dintre aceştia, vizează şi vulnerabilităţile detectate.

Procedurile pentru managementul evenimentelor/incidentelor/vulnerabilităţilor vizează şi incidentele cibernetice în cazul a 11 furnizori, pentru alţi 4 furnizori există proceduri distincte pentru astfel de incidente.

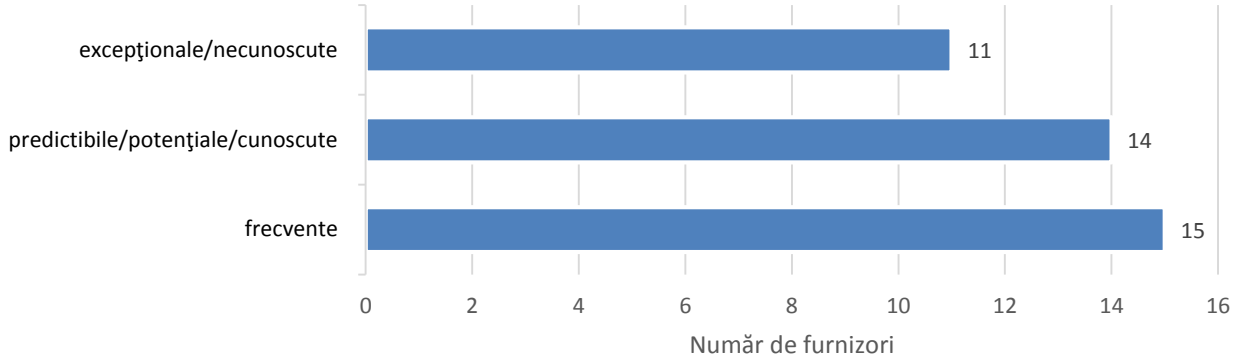
În majoritatea cazurilor, procedurile privind managementul incidentelor acoperă procesele de detectare şi raportare internă, evaluare/triere şi decizie, răspuns, escaladare, colectare a informaţiilor despre incidente şi păstrarea evidenţei acestora. 2 furnizori au afirmat că procedurile nu acoperă procesul de răspuns.

Procedurile privind managementul incidentelor cuprind şi definirea, respectiv alocarea rolurilor şi responsabilităţilor persoanelor adecvate pentru 15 furnizori.

În rândul celor 16 furnizori chestionaţi, procedurile privind managementul incidentelor acoperă cazul incidentelor frecvente pentru 15 furnizori, predictibile/potenţiale/cunoscute pentru 14 furnizori şi excepţionale/necunoscute pentru 11 furnizori (figura 9). Conform răspunsurilor primite,

aceste proceduri acoperă toate cele 3 cazuri (incidente frecvente, predictibile/potenţiale/cunoscute şi excepţionale/necunoscute) pentru 9 furnizori.

Fig.9 Procedurile privind managementul incidentelor acoperă cazul incidentelor:



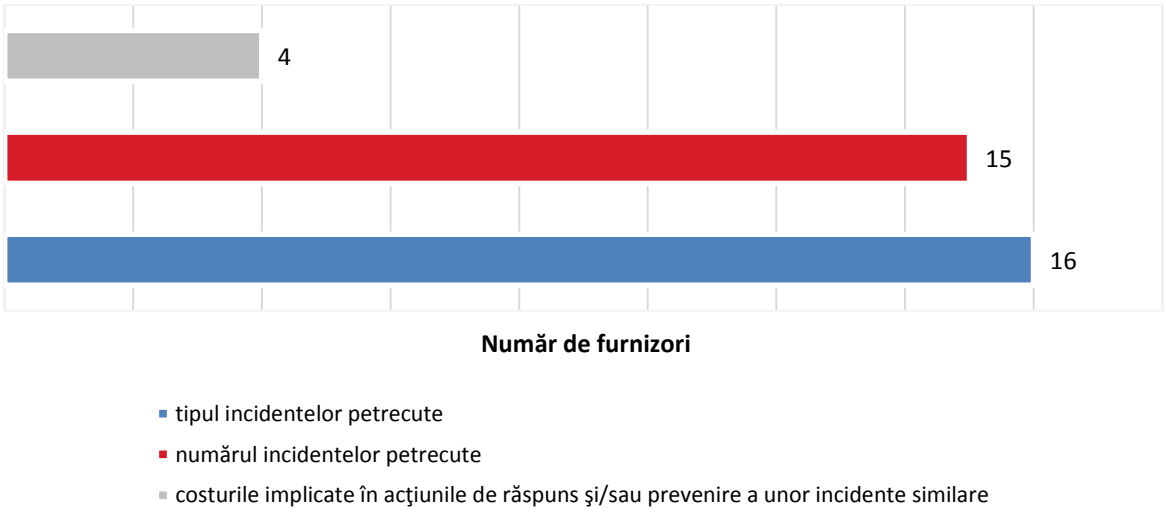
Potrivit răspunsurilor primite, procedurile privind managementul incidentelor stabilite în cadrul organizaţiilor furnizorilor chestionaţi descriu procesele şi fluxurile ce trebuie aplicate/urmate în cazul apariţiei incidentelor.

De regulă, procedurile delimitează diferite tipuri de evenimente/incidente în funcţie de nivelul de criticitate, de resursele ce pot fi afectate sau de părţile implicate în tratarea/remedierea acestora (deranjamente apărute în infrastructura de comunicaţii electronice, incidente de securitate a informaţiilor, incidente critice/majore, incidente apărute pe sisteme IT interne sau externalizate, sesizări primite din partea clienţilor, incidente a căror rezolvare necesită implicarea furnizorilor de echipamente etc.).

4. Evaluarea schemei de management al incidentelor şi îmbunătăţiri

Toţi furnizorii deţin metode/instrumente/mecanisme pentru determinarea/măsurarea şi monitorizarea tipului incidentelor petrecute. Doar 4 furnizori au instrumente de determinare/măsurare şi monitorizare a costurilor implicate în acţiunile de răspuns şi/sau prevenire a unor incidente similare (figura 10).

Fig.10 Există metode/instrumente/mecanisme pentru a determina/măsura şi monitoriza:



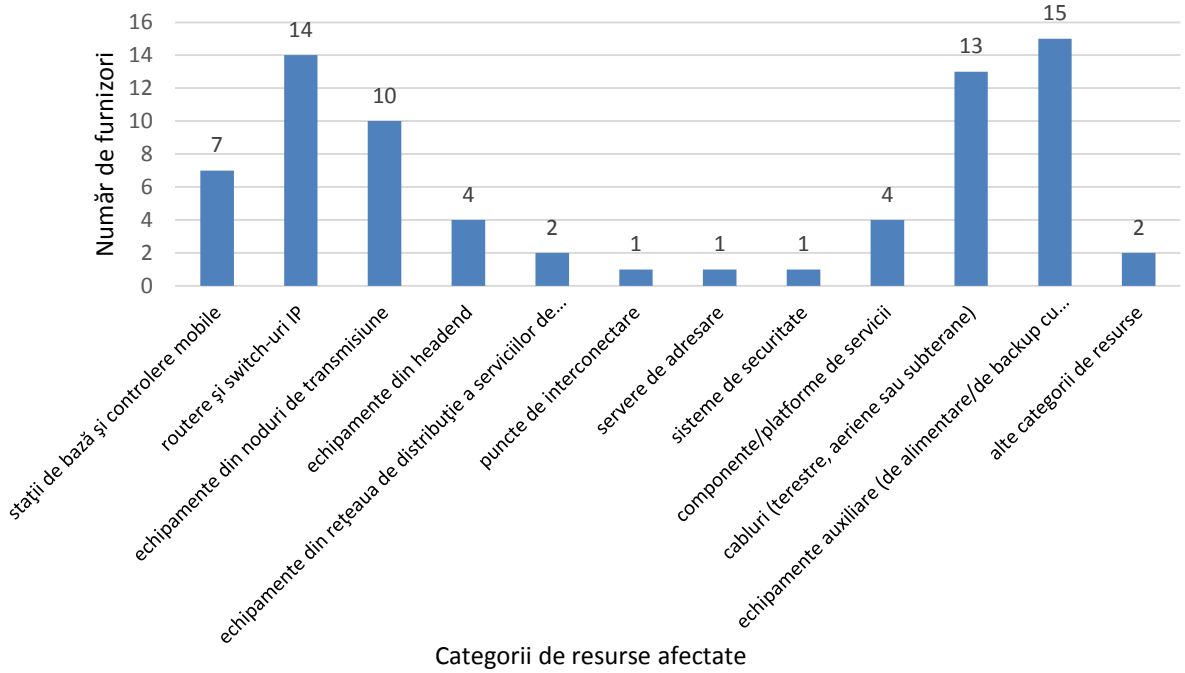
Astfel de instrumente constau de exemplu în rapoarte periodice privind incidentele, sisteme de ticketing electronic ce permit urmărirea tuturor incidentelor de la apariţie până la remediere, analize statistice, software dedicat pentru managementul incidentelor.

Durata medie a incidentelor este un bun indicator al impactului lor. Valoarea medie a acestui indicator calculată pentru 11 furnizori care au oferit informaţii relevante în acest sens este de 5 ore şi 30 de minute.

Printre cauzele frecvente ale incidentelor au fost menţionate: probleme de alimentare cu energie electrică/lipsa tensiunii în reţea/întreruperi şi defecţiuni ale surselor de alimentare cu energie electrică, condiţii meteorologice nefavorabile, lucrări efectuate de terţi, defectarea unor echipamente la nivel hardware, blocarea unor echipamente din cauza variaţiilor tensiunii electrice, vandalism, furturi şi distrugeri ale cablurilor de cupru şi fibră optică, erori umane (configurare de echipamente), infiltrarea unor viruşi. Cea mai frecventă cauză a incidentelor este reprezentată de problemele referitoare la alimentarea cu energie electrică, astfel de probleme fiind menţionate de 13 dintre furnizorii chestionaţi.

Furnizorilor li s-a solicitat să selecteze dintr-o listă de 19 categorii de resurse ce pot fi afectate de incidente, primele 5 categorii care sunt cel mai frecvent afectate. Astfel, cel mai frecvent afectate categorii de resurse sunt echipamente auxiliare (de alimentare/de backup cu energie electrică, sisteme de răcire etc.), routere şi switch-uri IP, cabluri (terestre, aeriene sau subterane).
Staţiile de bază şi controlerele mobile, precum şi echipamentele din noduri de transmisiune sunt de asemenea frecvent afectate de incidente (figura 11).

Fig.11 Categoriile de resurse afectate frecvent de incidente



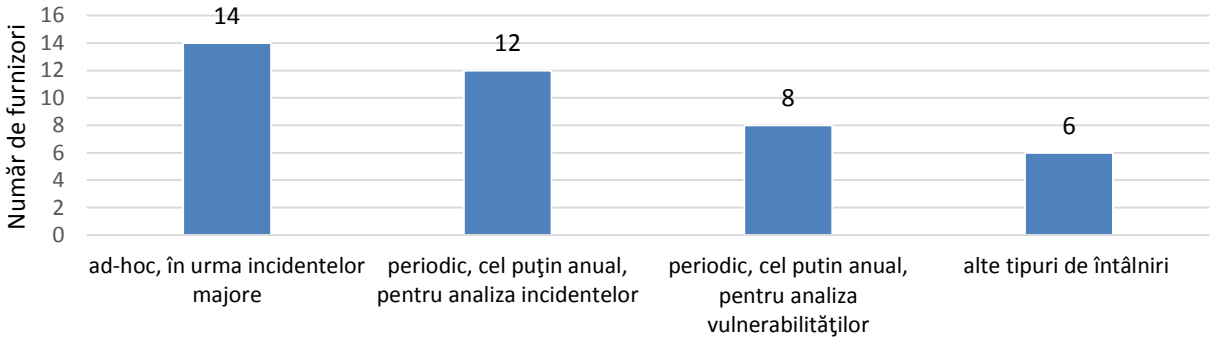
4.1 Analiza incidentelor şi organizarea unor întâlniri

În ceea ce priveşte analiza evenimentelor/incidentelor/vulnerabilităţilor, 14 organizaţii analizează periodic informaţiile din rapoartele individuale/baza de date ale/a incidentelor pentru a identifica tendinţele incidentelor şi domeniile ce necesită atenţie specială şi pentru a evalua măsurile ce pot fi luate pentru prevenirea unor incidente similare, 10 organizaţii analizează periodic vulnerabilităţile şi numai 3 organizaţii întocmesc rapoarte anuale cu situaţia incidentelor petrecute.

Frecvenţa analizei informaţiilor despre incidente pe parcursul lui 2014 variază în rândul furnizorilor. Astfel, aceştia analizează informaţiile din rapoartele individuale/baza de date ale/a incidentelor săptămânal, lunar, trimestrial sau ori de câte ori se înregistrează evenimente speciale.

Cei mai mulţi furnizori organizează întâlniri ad-hoc, în urma incidentelor majore, între membrii echipei de răspuns/personalul responsabil cu managementul/tratarea incidentelor, în care se analizează incidentul respectiv. 12 furnizori organizează întâlniri periodic, cel puţin anual, între membrii echipei de răspuns/personalul responsabil cu managementul/tratarea incidentelor, în care analizează incidentele înregistrate pe o anumită perioadă anterioară şi 8 furnizori organizează întâlniri periodic, cel puţin anual, între membrii echipei de răspuns/personalul responsabil cu managementul/tratarea incidentelor, în care analizează vulnerabilităţile detectate. Conform răspunsurilor primite, printre întâlnirile organizate în scopul analizei incidentelor se află şi întâlniri de tipul: întâlniri operaţionale săptămânale, întâlniri cu vendorii de echipamante, cu echipele de inginerie, întâlniri organizate imediat după incident, precum şi lunar în cadrul cărora se fac analize şi planuri de măsuri pentru evitarea repetării unor incidente similare, întâlniri interdepartamentale (figura 12).

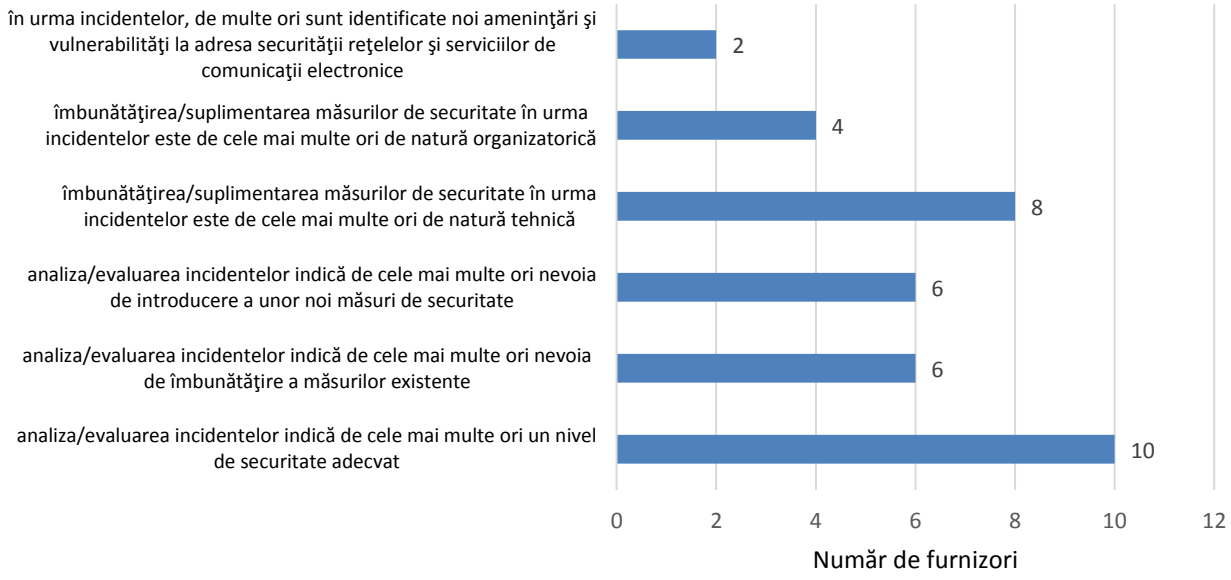
Fig.12 Întâlniri în urma incidentelor



4.2 Deprinderea unor lecţii în urma incidentelor şi îmbunătăţiri asupra măsurilor de securitate

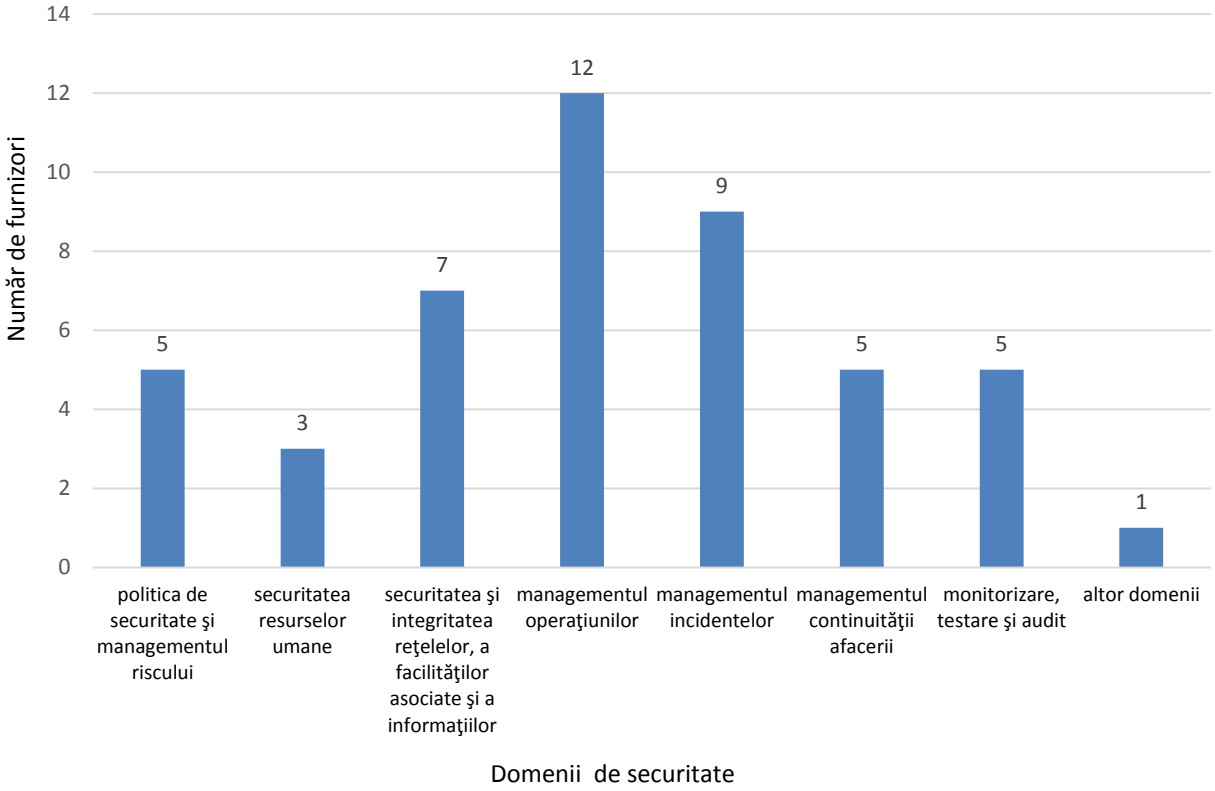
Graficul de mai jos prezintă o imagine de ansamblu asupra necesităţii de îmbunătăţire a măsurilor de securitate în urma incidentelor, în rândul furnizorilor chestionaţi.

Fig. 13 Îmbunătăţiri asupra măsurilor de securitate



Managementul operaţiunilor este domeniul ce necesită de cele mai multe ori îmbunătăţiri în urma incidentelor, urmat de domeniul managementului incidentelor (figura 14).

Fig.14 De obicei, îmbunătăţirile necesare în urma incidentelor aparţin unor domenii precum:



Printre exemplele de îmbunătăţiri/măsuri ce au fost aplicate de furnizorii chestionaţi pe parcursul anului curent au fost menţionate următoarele:

- revizuirea unor politici şi/sau proceduri ale organizaţiei;
- ajustarea/revizuirea modelelor de raportare;
- condiţii noi pentru testarea şi verificarea candidaţilor pentru angajare;
- schimbarea politicii parolelor;
- limitarea accesului în cadrul organizaţiei;
- clasificarea drepturilor de acces la baze de date în funcţie de ierarhie şi organigramă;
- achiziţionarea de echipamente de *backup*;
- instalarea unor sisteme de securitate;
- întocmirea unui plan de continuitate a afacerii;
- implementarea de noi standarde de securizare a echipamentelor;
- verificarea securităţii echipamentelor existente;
- îmbunatăţirea securităţii site-urilor prin aplicarea de măsuri anti-vandalizare, sisteme redundante pentru alimentarea cu energie electrică, optimizarea rutelor de transport;
- întâlniri lunare între managerii regionali şi managerii de la nivel central;
- definirea unui nou mod de lucru pentru a asigura un *SLA* mai bun în rezolvarea incidentelor;
- refacerea politicii de acces *remote* pentru tot personalul tehnic;
- implementarea unei aplicaţii pentru managementul incidentelor;
- măsuri privind continuitatea afacerii (de exemplu multiplicarea unor resurse centralizate pentru asigurarea funcţionării serviciilor în cazul evenimentelor majore din *datacenter*-ul organizaţiei);

- dotarea *headend*-urilor cu echipamente de aer condiţionat;
- detalierea activităţilor desfăşurate în teren de către subcontractori;
- dezvoltarea unor aplicaţii interne de monitorizare;
- asigurarea politicii de *health and safety*;
- efectuarea de audituri tehnice în reţea;
- securizarea mecanică suplimentară a suporţilor de comunicaţii.

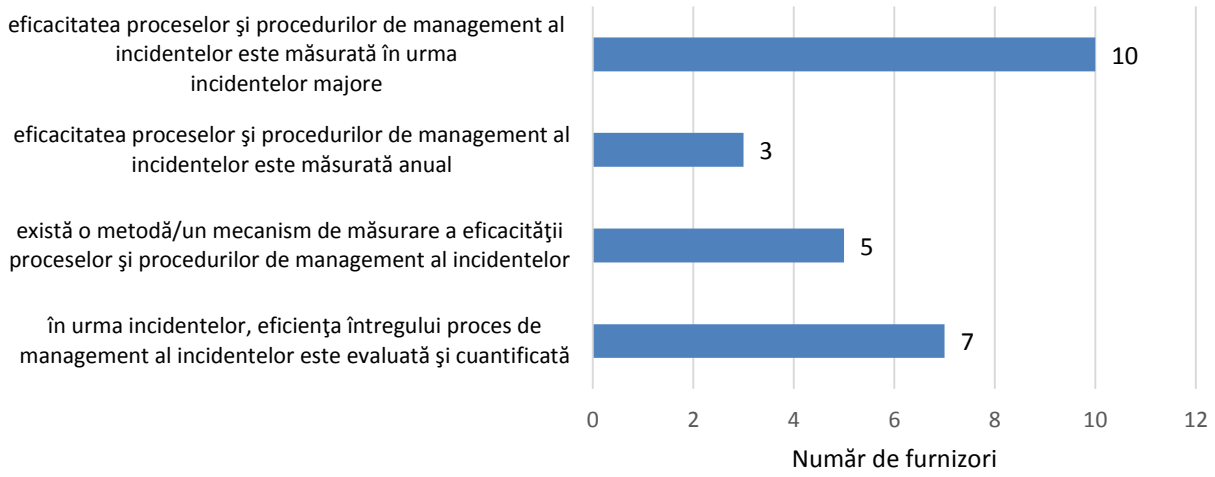
11 furnizori au afirmat că există/au existat îmbunătăţiri/măsuri de securitate specifice incidentelor cibernetice.

10 furnizori au dat exemple de măsuri specifice incidentelor cibernetice, aplicate în cadrul propriilor organizaţii. Astfel de măsuri au vizat:

- îmbunătăţirea proceselor de autentificare pe echipamente;
- campanii de conştientizare a ameninţărilor;
- implementarea unei platforme dedicate pentru monitorizarea traficului de internet şi detectarea de atacuri de tip *Denial of Service* (*DoS*);
- restricţionarea accesului în sisteme;
- modificarea pragurilor de detecţie şi a parametrilor de minimizare a impactului pentru atacurile de tip *DDoS*;
- monitorizarea alertelor de la antiviruşi, a logurilor de la *firewall* etc.;
- crearea unor noi reguli în cadrul sistemului de *intrusion/prevention;*
- *update*-uri de securitate pe sistemele expuse public;
- scanarea periodică a vulnerabilităţilor etc..

Graficul de mai jos ilustrează preocuparea furnizorilor asupra evaluării şi măsurării eficienţei proceselor şi procedurilor privind managementul incidentelor.

Fig.15 Măsurarea eficienţei/eficacităţii managementului incidentelor



Majoritatea furnizorilor au descris pe scurt metoda/mecanismul de măsurare a eficacităţii proceselor şi procedurilor de management al incidentelor.

Printre metodele menţionate se regăsesc următoarele:

- urmărirea rapoartelor incidentelor, monitorizarea repetabilităţii cauzei pentru incidentele viitoare, eliminarea repetabilităţii unor incidente similare şi evitarea apariţiei altor incidente corelate;

- măsurarea timpilor de remediere a incidentelor în vederea diminuării acestora, inclusiv identificarea etapelor/echipelor implicate cu un timp de răspuns mai mare decât cel agreat sau cu variaţii de la procesul agreat;

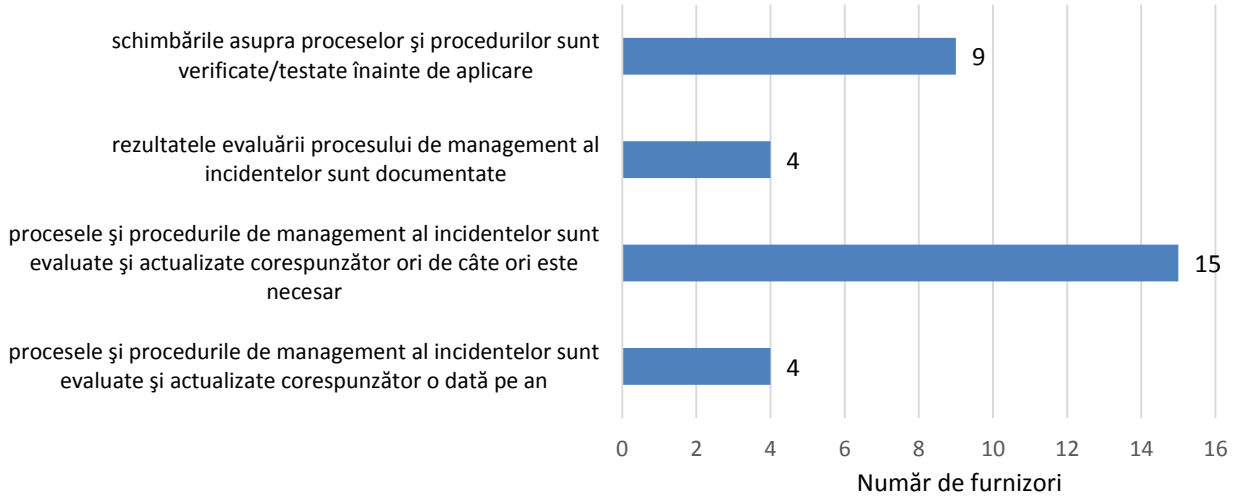
- măsurarea unor indicatori de performanţă operaţională, organizatorică, administrativă şi a gradului de îndeplinire a indicatorilor/obiectivelor prestabilite;

- organizarea unor întâlniri pentru analiza eficienţei proceselor, analiza rapoartelor incidentelor şi dispunerea unor măsuri de corecţie/modificare a proceselor şi procedurilor;

- audit intern *SMSI*[11] şi analiză *SMSI*.

Figura 16 prezintă interesul manifestat de furnizori în ceea ce priveşte evaluarea şi actualizarea managementului incidentelor.

Fig.16 Evaluarea şi actualizarea managementului incidentelor



Din grafic se observă un interes scăzut din partea furnizorilor asupra documentării rezultatelor evaluării procesului de management al incidentelor.

Majoritatea furnizorilor evaluează şi actualizează procesele şi procedurile de management al incidentelor ori de câte ori este necesar, 4 furnizori au afirmat că frecvenţa actualizărilor este anuală.

II. Sistem de detectare a incidentelor

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

Furnizorii au fost rugaţi să enumere sistemele de detectare a evenimentelor/incidentelor ce afectează/pot afecta furnizarea reţelelor şi serviciilor de comunicaţii electronice. Majoritatea furnizorilor au indicat sisteme specifice pentru monitorizarea şi managementul reţelelor. Unii furnizori au enumerat şi sisteme ce contribuie la sporirea securităţii fizice. Printre sistemele enumerate se regăsesc:

- sisteme de monitorizare şi alertare pentru reţele, servicii, echipamente, aplicaţii (de exemplu sisteme de monitorizare a echipamentelor active de reţea acces şi backbone, aplicaţii interne de tip *OSS* (*Operational Support Systems*), instrumente de monitorizare a performanţei reţelei, aplicaţii de măsurare a traficului de reţea, sisteme de monitorizare a platformelor specifice diferitelor tehnologii,

sistem de monitorizare a fibrei optice şi a echipamentelor pentru transport radio etc.);

[11] Sistem de Management al Securității Informației

- utilizarea de senzori, roboţi;

- sisteme software de corelare a evenimentelor;

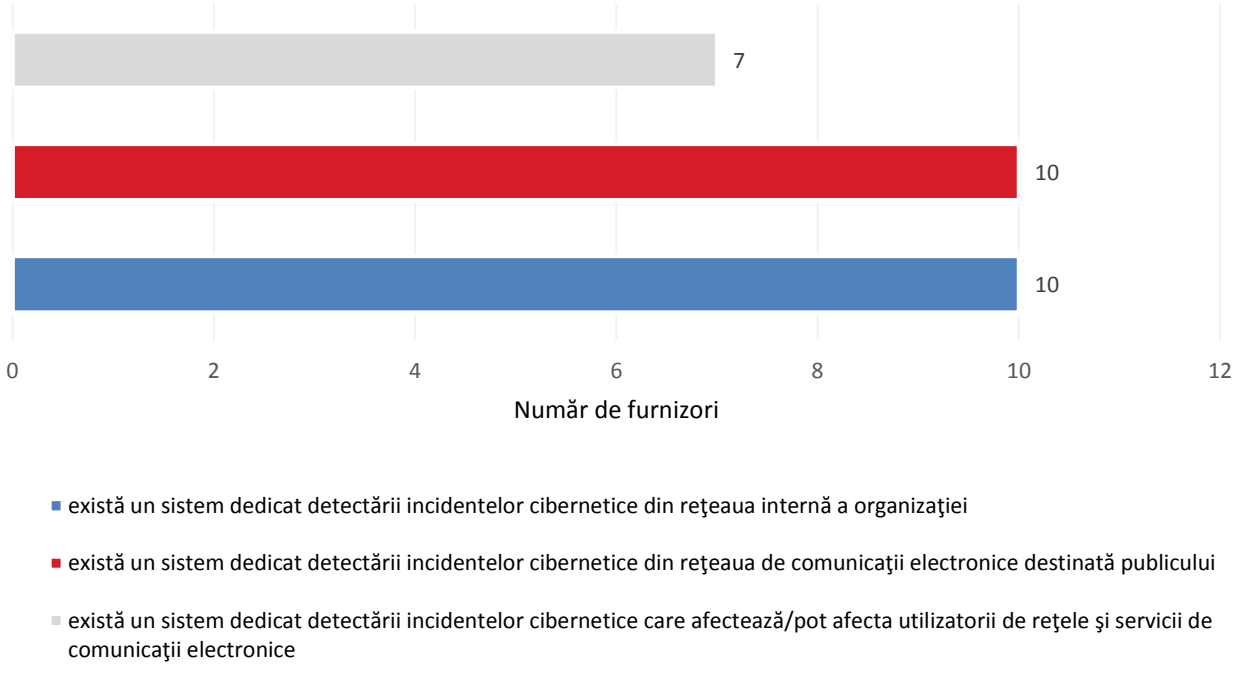
- sisteme de monitorizare/control al accesului fizic la *data centere, site-uri* etc.;

- sisteme auxiliare (pentru monitorizarea prezenţei energiei electrice, de climatizare, pentru stingerea incendiilor etc.);

- sisteme de securitate (*firewall*, detectare *spam-uri*, detectare atacuri de tip *DDoS*).

Majoritatea furnizorilor deţin capabilităţi pentru detectarea incidentelor cibernetice. Aceste capabilităţi sunt cuprinse în cadrul sistemelor de detectare a evenimentelor/incidentelor din cadrul organizaţiei (pentru 7 dintre furnizorii chestionaţi) sau sunt separate în sisteme dedicate acestui tip de incidente (figura 17).

Fig. 17 Sisteme pentru detectarea incidentelor cibernetice



1. Tipuri de detectare

Din punct de vedere al momentului detectării (înainte sau după producerea evenimentului/incidentului), majoritatea furnizorilor au sisteme/instrumente atât pentru detectarea proactivă, cât şi pentru detectarea reactivă a evenimentelor/incidentelor. Astfel, 4 furnizori au afirmat că deţin sisteme/instrumente doar pentru detectarea reactivă a evenimentelor/incidentelor şi 12 furnizori au afirmat că în cadrul organizaţiilor lor există sisteme/instrumente atât pentru detectarea reactivă, cât și pentru detectarea proactivă a evenimentelor/incidentelor.

În unele cazuri, aceleaşi sisteme au capabilităţi pentru ambele tipuri de detectare.

Printre sistemele/instrumentele enumerate pentru detectarea proactivă a evenimentelor/incidentelor, se regăsesc:

- sisteme/instrumente de monitorizare/supervizare a reţelelor, serviciilor, echipamentelor, aplicaţiilor, pentru monitorizarea parametrilor de performanţă/calitate a reţelelor şi/sau serviciilor etc;

- senzori, roboţi;

- instrumente de monitorizare a utilităţilor (de exemplu monitorizarea temperaturii şi/sau umidităţii, monitorizarea funcţionării *UPS*-urilor şi alarmare în cazul lipsei tensiunii de alimentare a acestor sisteme);

- sisteme de monitorizare a încărcării reţelei, a capacităţii de procesare a echipamentelor.

Detectarea proactivă a evenimentelor/incidentelor implică şi acţiuni precum:

- verificări periodice ale stării nodurilor reţelei;

- verificarea notificărilor primite de la vendori cu posibile erori;

- analize de trend ale problemelor detectate reactiv.

În continuare se regăsesc exemple de sisteme/instrumente enumerate de furnizori pentru detectarea reactivă a evenimentelor/incidentelor:

- sisteme de supervizare şi management al reţelei (de exemplu sisteme „tip umbrelă" de management al reţelei);

- aplicaţii interne pentru monitorizare şi alertare (de tip *OSS*, *Cacti,* soluţii *O&M* etc.);

- sisteme de detectare a unor tipuri de atacuri (*DDoS*, *flood*);

- aplicaţia de *ticketing* a organizaţiei;

- unelte de evaluare a parametrilor de calitate a serviciilor;

- reclamaţiile abonaţilor.

2. Monitorizarea funcţionării reţelelor şi serviciilor de comunicaţii electronice

2.1. Necesitatea monitorizării/resurse monitorizate

Printre resursele ce sunt monitorizate (atât din punct de vedere fizic, cât şi logic) în vederea detectării incidentelor ce pot afecta furnizarea reţelelor şi serviciilor de comunicaţii electronice, se numără:

- locaţii ce aparţin organizaţiei (de exemplu centre de date);

- echipamente ale reţelelor de comunicaţii electronice (de exemplu echipamente active ale reţelei de acces, echipamente de tip *backbone* - switch-uri, routere, servere etc.);

- componente ale unor echipamente (resurse de procesare, memorie etc.);

- echipamente instalate la client (*CPE*);

- resurse informatice precum baze de date, aplicaţii, sisteme de operare;

- echipamente conexe sau auxiliare care permit funcţionarea reţelelor (de exemplu monitorizarea prezenţei energiei electrice/*UPS*-uri, sisteme de climatizare, sisteme pentru stingerea incendiilor, monitorizarea temperaturii *site*-urilor);

- cabluri.

2.2. Primirea sesizărilor/indiciilor/notificărilor despre incidente din partea unor persoane

Pentru cea mai mare parte a furnizorilor chestionaţi, evenimentele/incidentele ce pot afecta/afectează furnizarea reţelelor şi serviciilor de comunicaţii electronice pot fi detectate şi pe baza unor sesizări/informări din partea personalului organizaţiei, din partea unor părţi externe precum organizaţii de profil/parteneri de afaceri, altor furnizori de reţele şi servicii de comunicaţii electronice, precum şi din partea utilizatorilor de reţele şi servicii de comunicaţii electronice.

Evenimentele/incidentele/vulnerabilităţile sunt notificate intern prin intermediul comunicării directe/verbale, prin e-mail, fax, telefon, prin intermediul alarmelor, folosind platforme de *ticketing*

pentru înregistrarea incidentelor/deschiderea unor sesizări, prin informarea *NOC*-ului, a turelor de monitorizare a funcţionării sistemelor, a şefului direct. Unii furnizori au menţionat că informări succinte despre apariţia incidentelor sunt transmise şi departamentului organizaţiei responsabil cu informarea utilizatorilor de servicii de comunicaţii electronice.

De cele mai multe ori, părţile externe indică/notifică evenimente/incidente/vulnerabilităţi telefonic şi/sau prin e-mail. Unii furnizori au indicat sistemul de *ticketing*, informarea *NOC*-ului sau serviciul de relaţii cu clienţii ca modalităţi utilizate în acest scop.

În rândul furnizorilor chestionaţi, utilizatorii de reţele şi servicii de comunicaţii electronice indică/sesizează evenimente/incidente/vulnerabilităţi telefonic (de regulă prin intermediul serviciului de relaţii cu clienţii – *call center*) şi prin e-mail. Alte mijloace menţionate în acest sens sunt faxul, poşta, mediul online (de exemplu reţelele de socializare).

2.3. Primirea sesizărilor/indiciilor/notificărilor despre incidente de la echipamente/sisteme

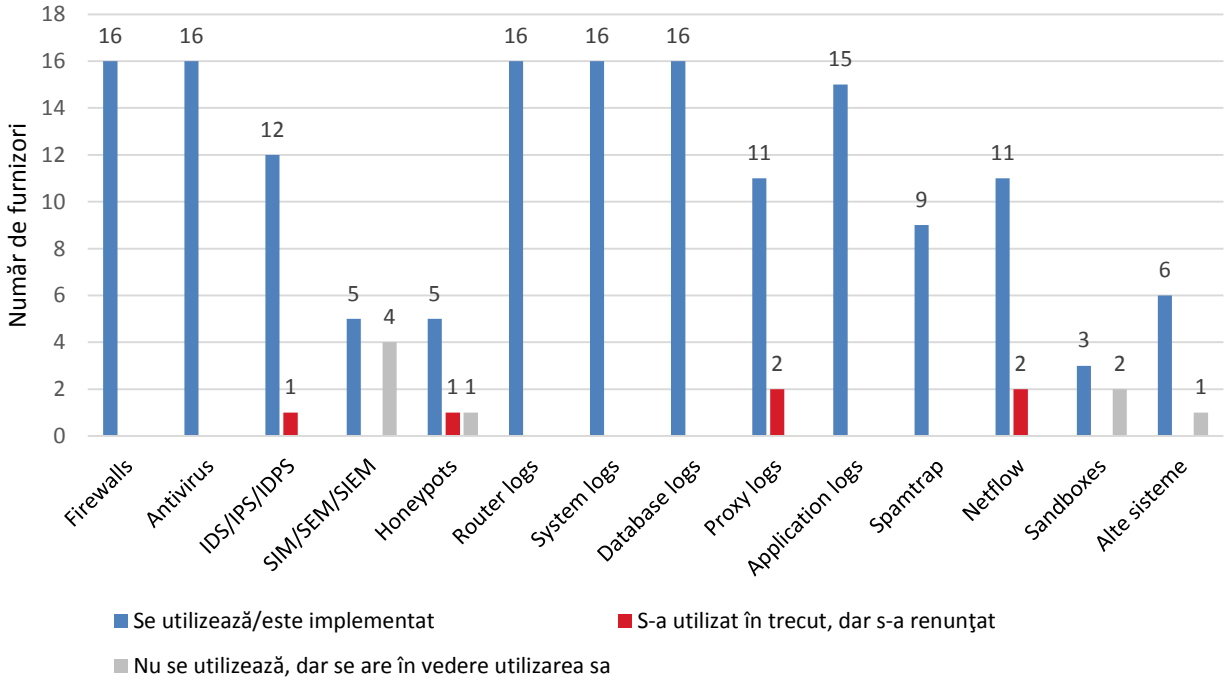
2.3.1 Monitorizarea reţelei interne/sistemelor informatice

În cadrul chestionarului s-a făcut distincţia între reţeaua de comunicaţii electronice şi reţeaua internă a organizaţiei. Furnizorii au afirmat că monitorizează reţeaua internă a organizaţiei. Majoritatea răspunsurilor la întrebarea dedicată descrierii procesului/modalităţilor de monitorizare a reţelei interne a organizaţiei au fost concentrate pe soluţii de monitorizare specifice (de exemplu aplicaţie software dedicată cu alertare în cazul incidentelor, soluţie integrată de monitorizare, *gateway* prin care este administrată reţeaua internă, soft-uri de management dedicate).

Răspunsurile au indicat faptul că nu au existat cazuri în care afectarea/compromiterea reţelei interne să conducă la afectarea furnizării reţelelor şi serviciilor de comunicaţii electronice.

Furnizorii au fost rugaţi să bifeze situaţiile aplicabile în ceea ce priveşte sistemele/instrumentele de detectare din cadrul propriilor organizaţii şi utilizarea acestora. Răspunsurile sunt ilustrate în figura 18.

Fig.18 Sisteme/instrumente de detectare şi utilizarea acestora



Aşa cum se observă şi din graficul anterior, toţi furnizorii chestionaţi utilizează *firewalls, antivirus* şi înregistrări la nivel de echipament de rutare, sistem, bază de date, aplicaţie *(router logs, system logs, database logs, application logs)* pentru detectarea evenimentelor/incidentelor. 12 furnizori utilizează *IDS/IPS/IDPS*[12] şi 1 furnizor a utilizat în trecut astfel de sisteme, dar a renunţat la ele. Doar 5 furnizori utilizează sisteme de tipul *SIM/SEM/SIEM*[13], însă alţi 4 intenţionează să implementeze în viitor sisteme de acelaşi tip. Sisteme precum *proxy logs* şi *netflow*[14] au un grad ridicat de utilizare, 11 dintre furnizori având implementate astfel de sisteme. Pe lângă instrumentele oferite drept exemple în cadrul chestionarului, 6 respondenţi au menţionat şi alte sisteme întrebuinţate în acelaşi scop. Interesul cel mai scăzut aparţine unor sisteme/instrumente precum *honeypots*[15] şi *sandboxes*[16].

2.3.2 Monitorizarea elementelor reţelei de comunicaţii electronice

Monitorizarea reţelei de comunicaţii electronice se realizează atât la nivel de reţea/serviciu, la nivel de echipamente distincte, cât şi la nivel de aplicaţii distincte pentru 11 dintre furnizorii chestionaţi. În cazul a 3 furnizori, monitorizarea reţelei de comunicaţii electronice se realizează doar la nivel de echipamente distincte, iar pentru ceilalţi 2 furnizori chestionaţi monitorizarea se realizează la nivel de reţea/serviciu şi la nivel de echipamente distincte.

Pentru 12 dintre furnizori există un proces de corelare a rezultatelor monitorizării echipamentelor/aplicaţiilor distincte.

Activităţile de monitorizare a reţelei/serviciilor/echipamentelor/aplicaţiilor sunt realizate de personalul organizaţiei pentru 10 furnizori. Pentru ceilalţi 6 furnizori aceste activităţi sunt realizate de personalul organizaţiei şi de alte părţi subcontractate.

Monitorizarea reţelei şi/sau a elementelor/echipamentelor reţelei de comunicaţii electronice se realizează local şi la distanţă în cazul a 12 furnizori, pe când 4 furnizori desfăşoară activităţile de monitorizare numai la distanţă.

Soluţiile/sistemele/aplicaţiile utilizate de furnizorii respondenţi pentru monitorizarea elementelor/echipamentelor reţelei de comunicaţii electronice se referă în principiu la sisteme de management integrate în sisteme de tip "umbrelă", de tip *OSS*, *NMS* etc.. Conform răspunsurilor, soluţiile de monitorizare au fost achiziţionate de la diferiţi producători sau au fost dezvoltate intern.

Acţiunile de monitorizare şi gestionare a incidentelor din cadrul reţelei de comunicaţii electronice sunt realizate de către Centrul de Operaţiuni de Reţea (*NOC*) al fiecărei organizaţii pentru majoritatea furnizorilor chestionaţi.

Monitorizarea reţelei de comunicaţii electronice în vederea detectării evenimentelor/incidentelor ce afectează/pot afecta procesul furnizării reţelelor şi serviciilor de comunicaţii electronice este o atribuţie considerabilă/centrală în sfera de activitate a unui *NOC.*

---

[12] Un *IDS* este un sistem informatic utilizat pentru identificarea unor încercări de intruziuni, intruziuni ce au sau au avut loc şi eventual pentru răspunsul la intruziuni în reţele şi sisteme informatice. Un IPS este similar cu un IDS, dar lucrează de obicei în modul activ – este capabil să blocheze comportamentul maliţios. Sistemele IDPS sunt sisteme hibride ce înglobează capacităţi de detectare şi prevenire (IDS şi IPS).

[13] *SIEM (Security Information and Event Management*) reprezintă acel software de analiză a evenimentelor de securitate şi a comportamentelor anormale din reţea ce sunt extrase din jurnalele aplicaţiilor, sistemelor şi echipamentelor din reţea. *SIEM* implică colectarea, arhivarea, analiza, corelarea şi raportarea informaţiilor obţinute de la toate resursele eterogene ale reţelei. Tehnologia SIEM se află la intersecţia dintre *SIM (Security Information Management)* şi *SEM (Security Event Management*).

[14] *NetFlow* este un protocol de reţea dedicat colectării, monitorizării şi analizei traficului IP în vederea identificării incidentelor potenţiale, permiţând detectarea proactivă a incidentelor.

[15] Un *honeypot* reprezintă o capcană pentru detectarea şi urmărirea încercărilor de utilizare neautorizată a serviciilor reţelei sau a întreg sistemului de operare. Poate fi o parte izolată a unui sistem de operare (de exemplu server *SSH*) sau un sistem (de exemplu virtualizat). Se comportă ca un sistem de avertizare timpurie şi colectează informaţiile privind tendinţele atacurilor.

[16] *Sandbox* este un mediu în care un cod suspicios sau o aplicaţie pot rula izolat fără să afecteze un sistem de operare (mediul acesta este separat de sistemul de operare).

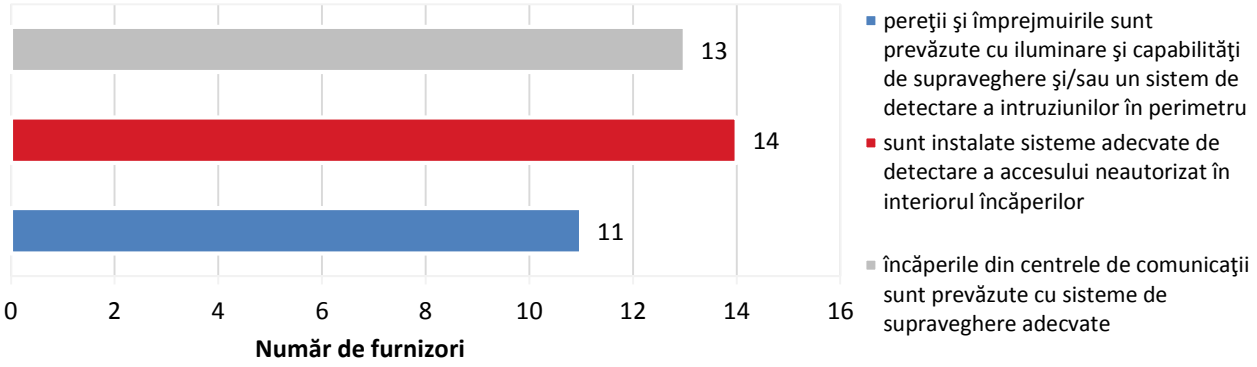
Conform răspunsurilor primite, printre acţiunile/activităţile principale ale *NOC*-ului în ceea ce priveşte managementul incidentelor, inclusiv din punct de vedere al monitorizării reţelei de comunicaţii electronice şi a infrastructurii asociate, se numără:

- monitorizarea sistemelor de management al reţelei 24/7/365 (monitorizarea segmentelor de *backhaul* şi a staţiilor de bază, monitorizarea echipamentelor de *backbone* şi a liniilor de fibră optică etc.);
- monitorizarea sistemelor ce asigură alimentarea electrică;
- identificarea tendinţelor traficului sau al încărcării nodurilor;
- detectarea, analiza şi urmărirea alarmelor prin sistemele de management;
- detectarea evenimentelor/incidentelor din reţea şi diagnosticarea acestora prin investigarea cauzelor;
- evaluarea impactului evenimentelor asupra eventualelor servicii afectate;
- notificarea interna a evenimentelor/incidentelor (de exemplu notificarea departamentelor de suport prin deschiderea de tichete ce sunt aduse la cunoştinţa celor vizaţi prin SMS, e-mail şi telefonic);
- comunicarea problemelor către alte părţi interesate;
- consemnarea evenimentelor în sistemul de tichetare, de unde sunt dispecerizate;
- urmărirea modului de rezolvare până la închiderea incidentului cu consemnarea etapelor urmate;
- managementul modificărilor în reţeaua de comunicaţii;
- remedierea incidentului sau escaladerea rezolvării către departamentul specializat (tehnic, IT etc.);
- aplicarea unor soluţii temporare sau finale în vederea restaurării serviciilor;
- documentare în privinţa incidentului (întocmirea raportului incidentului);
- propuneri pentru prevenirea incidentelor similare;
- rezolvarea incidentelor inclusiv cu posibile intervenţii în teren sau cu suport din partea altor părţi;
- investigaţii ale echipamentelor.

2.3.3 Monitorizarea locaţiilor

Răspunsurile la chestionar indică existenţa unor sisteme de detectare a incidentelor cauzate de accesul neautorizat în interiorul zonelor/clădirilor/centrelor de comunicaţii[17] în rândul furnizorilor chestionaţi. Figura 19 arată că un număr ridicat de furnizori au implementate măsuri în acest scop.

Fig.19 Măsuri pentru detectarea incidentelor cauzate de accesul neautorizat în interiorul zonelor/clădirilor/centrelor de comunicaţii



[17] Prin *zone/clădiri* se înţelege acele locaţii în care se desfăşoară activităţi specifice procesului de furnizare a reţelelor şi serviciilor de comunicaţii electronice. *Centrele de comunicaţii* sunt clădiri în care sunt concentrate echipamente esenţiale în procesul de furnizare a reţelelor şi serviciilor de comunicaţii electronice, ca de exemplu, centrele de comutaţie, centrele de control şi operare.

O măsură de securitate predominantă în rândul furnizorilor şi care sprijină procesul detectării incidentelor cauzate de accesul neautorizat în incinta organizaţiei este reprezentată de monitorizarea/supravegherea video. Astfel, printre sistemele de detectare a incidentelor cauzate de accesul neautorizat în interiorul zonelor/clădirilor/centrelor de comunicaţii au fost menţionate:

- sisteme de supraveghere (camere de supraveghere, de exemplu de tip *CCTV*[18], supraveghere electronică cu senzori de prezenţă etc.);

- pază cu agenţi de securitate (contract de servicii monitorizare cu firme de securitate sau pază proprie);

- sisteme de control acces/antiefracţie (de exemplu pe bază de cartele, turnichete, sisteme de incuietori specifice, sisteme bazate pe senzori, sisteme de avertizare sonoră, de monitorizare cu alarmă);

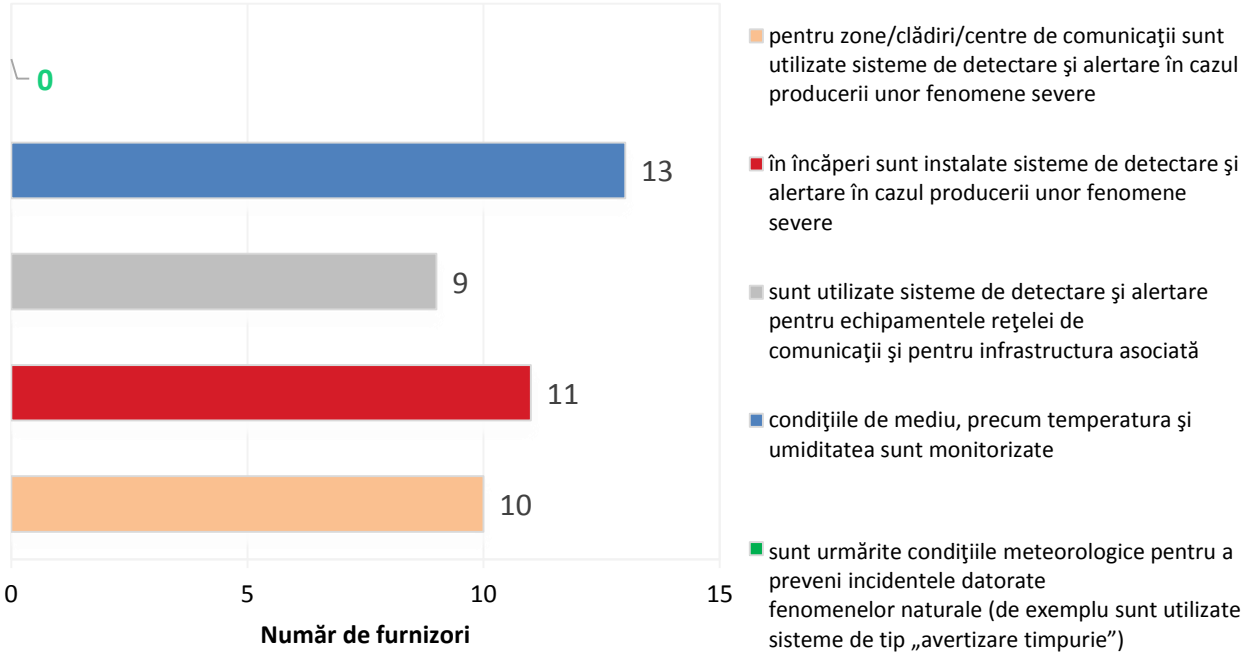
Potrivit răspunsurilor, unele sisteme mai complexe sunt instalate doar în anumite locaţii (sedii tehnice, centre de date, *PoP*[19]-uri mari).

Potrivit răspunsurilor, 10 furnizori monitorizează şi alte locaţii în care se află resurse ale organizaţiei în afară de zone/clădiri/centre de comunicaţii.

Printre alte locaţii indicate se numără zone izolate unde sunt amplasate *sheltere*, locaţii de tip *outdoor*, magazine din reţeaua de vânzări directe, sedii administrative.

Graficul următor indică existenţa unor măsuri pentru reducerea efectelor/declanşării/apariţiei unor fenomene severe pentru un număr ridicat de furnizori chestionaţi.

Fig.20 Măsuri pentru a reduce efectele declanşării/apariţiei unor fenomene severe



Se observă că nu există măsuri/capabilităţi (de exemplu sisteme de tip "avertizare timpurie") pentru urmărirea condiţiilor meteorologice în scopul prevenirii incidentelor cauzate de fenomene naturale.

[18] Closed circuit television
[19] Point of presence

3. Evaluarea şi actualizarea sistemului de detectare

7 furnizori au afirmat că evaluarea şi actualizarea sistemului de detectare a evenimentelor/incidentelor se realizează anual. Ceilalţi furnizori au menţionat o frecvenţă trimestrială, bianuală sau anuală, în timp real, lunar şi trimestrial, zilnic şi săptămânal sau ori de câte ori este nevoie.

Actualizarea sistemului/sistemelor de detectare ţine cont de schimbările înregistrate în cadrul reţelei şi de incidentele petrecute pentru 12 furnizori. 3 furnizori actualizează sistemul/sistemele de detectare ţinând cont doar de schimbările înregistrate în cadrul reţelei, iar în acelaşi scop, un furnizor are în vedere doar incidentele petrecute.

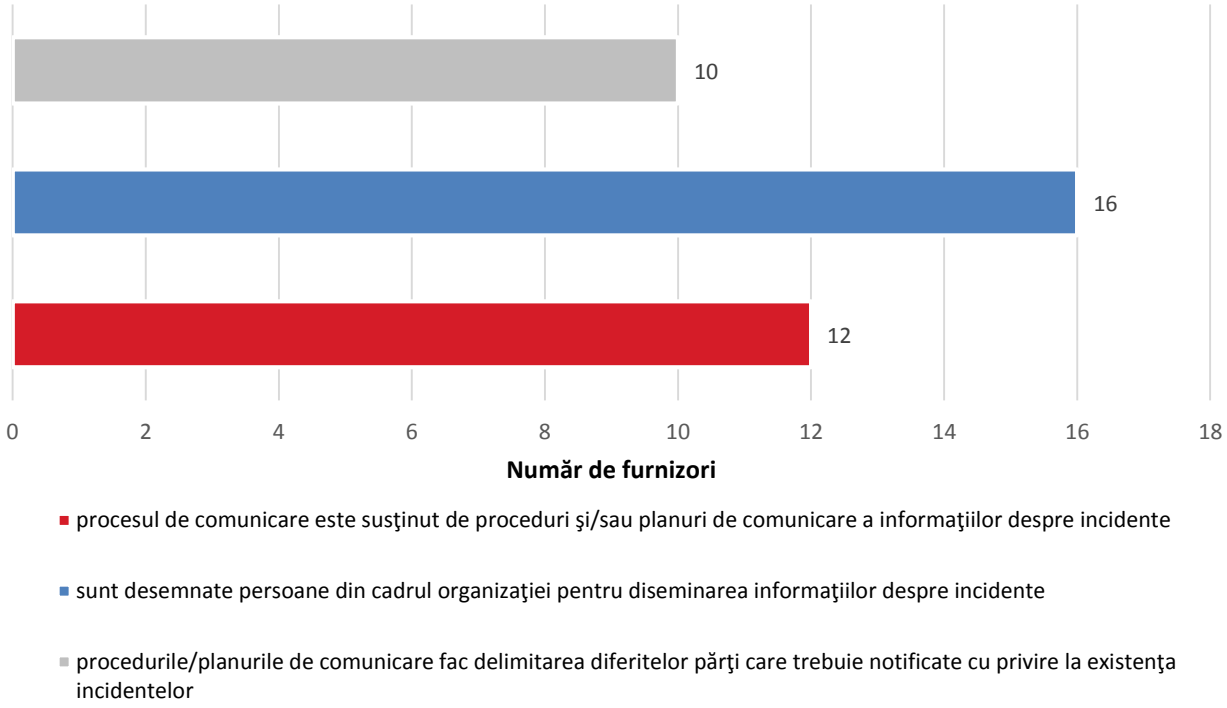
Din totalul incidentelor înregistrate în anul 2014, furnizorii au precizat că majoritatea incidentelor au fost detectate de sistemele/instrumentele de detectare proprii organizaţiei şi doar o mică parte a fost descoperită prin intermediul sesizărilor primite de la utilizatorii de reţele şi servicii de comunicaţii electronice.

III. Proceduri şi planuri de comunicare a incidentelor

Conform Deciziei nr.512/2013, furnizorii au obligaţia să stabilească o procedură adecvată de raportare a incidentelor către ANCOM, precum şi către alte autorităţi responsabile şi să stabilească planuri de comunicare a incidentelor către alte părţi externe (furnizori de reţele şi servicii de comunicaţii electronice afectaţi, media, clienţi, parteneri de afaceri etc.).

În ceea ce priveşte procedurile şi planurile de comunicare a informaţiilor despre incidente, 15 furnizori au afirmat că deţin un proces privind comunicarea informaţiilor despre incidente unor părţi externe. Procesul de comunicare este susţinut de proceduri şi/sau planuri de comunicare a informaţiilor despre incidente pentru 12 furnizori. Procedurile de comunicare a informaţiilor despre incidente includ formulare/template-uri specifice pentru 6 furnizori. Alte aspecte despre aceste proceduri şi planuri sunt prezentate grafic în continuare.

Fig.21 Proceduri şi planuri de comunicare a incidentelor



1. Proceduri de raportare a incidentelor către ANCOM, precum şi către alte autorităţi responsabile

Potrivit răspunsurilor oferite, majoritatea furnizorilor (14) au un proces de raportare a incidentelor către ANCOM, însă un număr restrâns (6) deţine proceduri specifice în care este detaliat acest proces.

Unii furnizori au descris succint procesul de raportare a incidentelor către ANCOM, punctând elementele principale ale procedurii de raportare stabilite de Autoritate prin Decizia nr.512/2013, alţii doar au indicat acest act normativ drept document de referinţă în privinţa procesului de raportare. 7 furnizori au oferit informaţii privind compartimentele sau persoanele din cadrul organizaţiei responsabile de raportarea incidentelor către ANCOM.

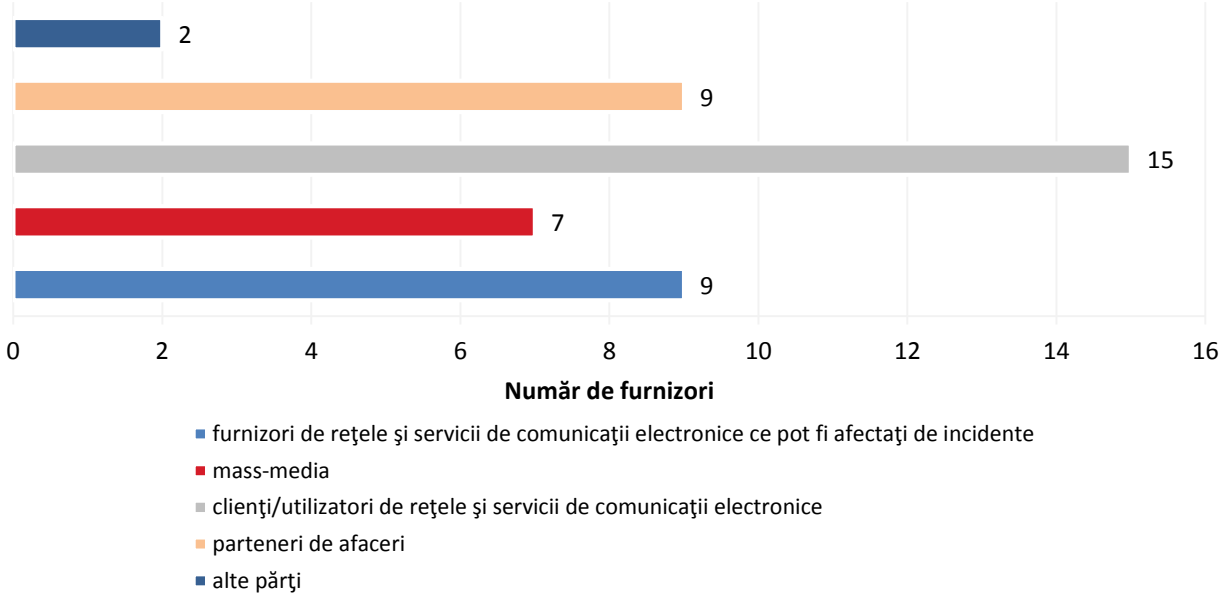
Conform răspunsurilor primite, dintre incidentele înregistrate pe parcursul anului 2014, 338 de incidente s-au încadrat pentru raportare către ANCOM (în total, pentru toţi furnizorii chestionaţi), luându-se în calcul incidentele petrecute de la începutul anului până la momentul elaborării răspunsului la chestionar. Majoritatea respondenţilor au ţinut să precizeze că raportarea s-a realizat în condiţiile stabilite prin Decizia preşedintelui ANCOM nr.512/2013. ANCOM deţine evidenţa incidentelor raportate de furnizori pe parcursul anului 2014, informaţii în acest sens vor fi publicate în *Raportul privind incidentele care au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice în anul 2014*.

În afară de ANCOM, 5 furnizori au menţionat că transmit informaţii despre incidente şi altor autorităţi/instituţii precum ANSPDCP[20] în cazul incidentelor care afectează integritatea datelor cu caracter personal (3 furnizori), CERT-RO[21] în cazul incidentelor cibernetice (1 furnizor) sau la solicitarea autorităţilor competente.

2. Planuri de comunicare către alte părţi privind incidentele

Următorul grafic arată în ce proporţie există planuri de comunicare a incidentelor către diferite grupuri de interes în rândul celor chestionaţi.

Fig.22 Există planuri de comunicare a incidentelor către:

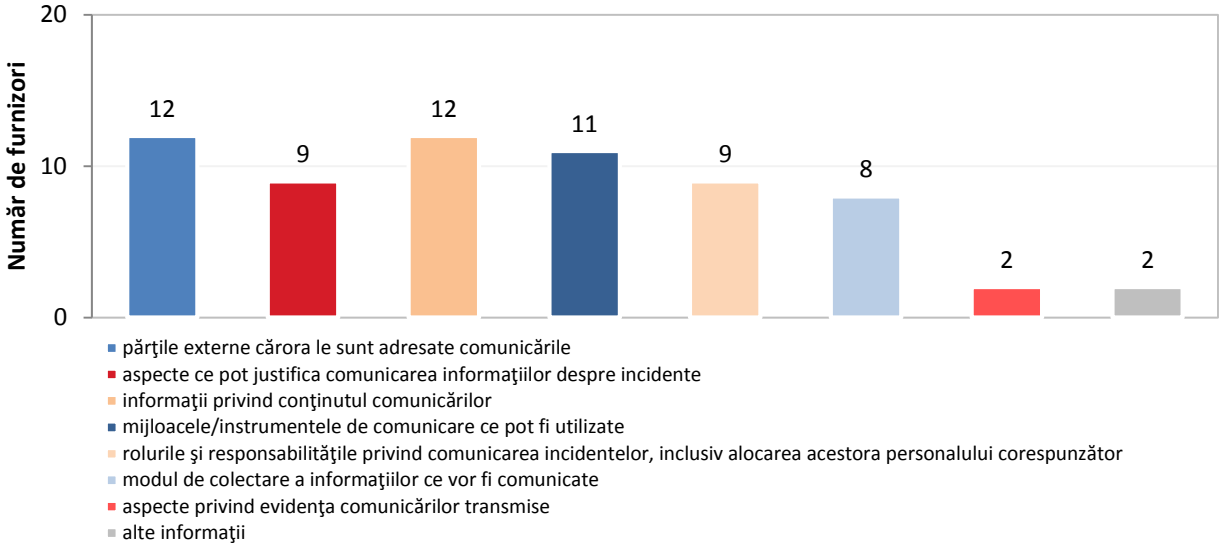


[20] Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal
[21] Centrul Național de Răspuns la Incidente de Securitate Cibernetică

Cu toate că doar 10 furnizori au afirmat că în cadrul propriilor organizaţii procedurile/planurile de comunicare fac delimitarea diferitelor părţi care trebuie notificate cu privire la existenţa incidentelor, 15 furnizori au informat asupra existenţei unor planuri de comunicare a incidentelor către clienţi/utilizatori de reţele şi servicii de comunicaţii electronice.

Figura 23 prezintă o situaţie în rândul respondenţilor a elementelor conţinute de planurile privind comunicarea informaţiilor despre incidente unor părţi externe organizaţiei.

Fig.23 Planurile privind comunicarea informaţiilor despre incidente unor părţi externe organizaţiei conţin:



Pentru majoritatea furnizorilor chestionaţi, descrierea planurilor de comunicare a incidentelor către părţi externe a constat în oferirea de informaţii în ceea ce priveşte elementele conţinute în cadrul informărilor şi modalităţile de informare întrebuinţate. Printre elementele planurilor de comunicare se regăsesc serviciile afectate, zona afectată, durata, cauza, timpul estimat de rezolvare.

Conform răspunsurilor, furnizorii nu au comunicat informaţii despre incidente altor furnizori de reţele şi servicii de comunicaţii electronice, mass-mediei şi nici partenerilor de afaceri pe parcursul lui 2014 sau nu deţin date statistice/o evidenţă cu privire la acest aspect.

Majoritatea furnizorilor chestionaţi (13 dintre aceştia) nu au indicat numărul informărilor transmise utilizatorilor de reţele şi servicii de comunicaţii electronice în anul 2014 privind incidentele ce au afectat securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

De regulă utilizatorilor le sunt comunicate incidentele cu prioritate mare (de exemplu căderile de serviciu care depăşesc 24 de ore, incidentele majore/critice).

Printre informaţiile ce sunt comunicate utilizatorilor în ceea ce priveşte existenţa unor incidente se regăsesc data producerii incidentului, durata de nefuncţionare a serviciului/termenul estimativ pentru remediere, tipul serviciilor afectate, aria geografică afectată de incident, informaţii privind apariţia unor vulnerabilităţi de securitate în reţeaua de comunicaţii electronice, măsurile ce trebuie luate de utilizatori în cazul incidentelor.

3. Modalităţi/instrumente de comunicare

Referitor la modalităţile/instrumentele de comunicare a informaţiilor despre incidente diverselor părţi externe, cei mai mulţi furnizori (12) comunică unele informaţii despre incidente nestandardizat, prin metode alese în funcţie de circumstanţele incidentului (comunicare ad-hoc). 7 furnizori utilizează formulare/template-uri specifice pentru facilitarea comunicării informaţiilor despre

incidente unor părţi externe. 4 furnizori au afirmat că au template-uri dedicate fiecărui gup ţintă căruia îi pot fi adresate informările despre incidente. Un singur furnizor diseminează informaţiile privind incidentele şi prin participarea personalului desemnat la conferinţe, întâlniri, dezbateri publice cu tematici în domeniu, iar 3 furnizori publică informaţii de interes pentru public în ceea ce priveşte incidentele petrecute.

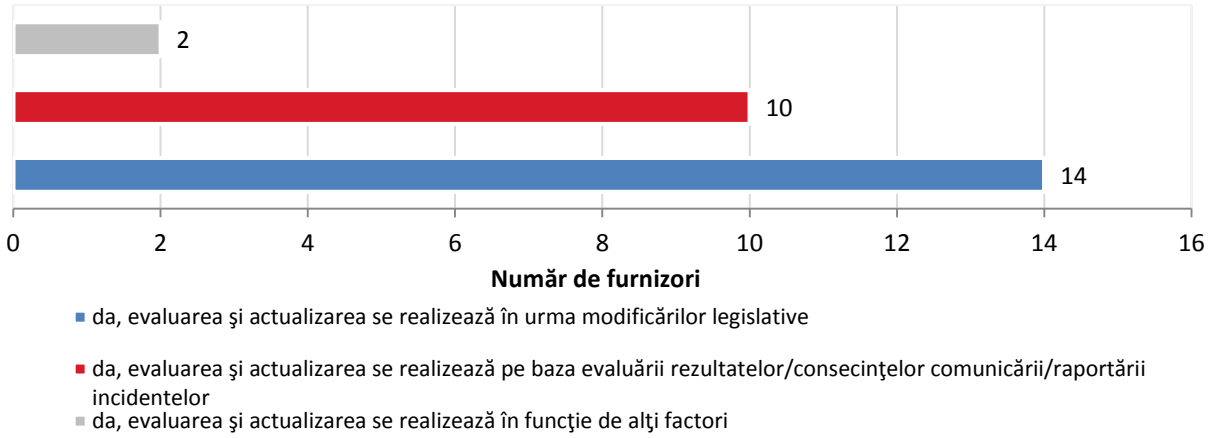
Printre mijloacele de informare a diverselor părţi externe se numără e-mailul, telefonul, website-ul organizaţiei, IVR-ul sau mass media după caz.

Pentru comunicarea informaţiilor despre incidente utilizatorilor de reţele şi servicii de comunicaţii electronice, furnizorii utilizează cel mai des mijloace/instrumente precum *call center*-ul, apelul telefonic, *IVR*-ul, e-mailul, SMS-ul. În cazul sesizărilor utilizatorilor finali comunicarea se realizează telefonic sau în scris; de cele mai multe ori, clienţii pot solicita informaţii despre un anumit incident telefonic, prin intermediul departamentului de relaţii cu clienţii.

4. Evaluarea şi actualizarea planurilor şi procedurilor de comunicare/raportare a incidentelor

Figura 24 se referă la procesul de evaluare şi actualizare a procedurilor şi/sau planurilor privind comunicarea/raportarea informaţiilor despre incidente unor părţi externe.

Fig.24 Există un proces de evaluare şi actualizare a procedurilor şi/sau planurilor privind comunicarea/raportarea informaţiilor despre incidente unor părţi externe?



2 furnizori au menţionat că evaluarea şi actualizarea procedurilor şi/sau planurilor privind comunicarea/raportarea informaţiilor despre incidente unor părţi externe se realizează pe baza rezultatelor auditurilor interne şi externe ale proceselor.

IV. Alte informaţii

În cadrul chestionarului, ANCOM a solicitat şi alte informaţii furnizorilor chestionaţi. Informaţiile de interes pentru Autoritate s-au referit la:

- tipurile de incidente care sunt cel mai greu de detectat şi remediat;

- problemele frecvente în ceea ce priveşte detectarea şi raportarea evenimentelor/incidentelor/vulnerabilităţilor, analiza, evaluarea, trierea incidentelor, răspunsul la incidente, inclusiv escaladarea, colectarea informaţiilor despre incidente şi păstrarea evidenţei acestora, comunicarea informaţiilor despre incidente unor părţi externe;

- tipurile de incidente cel mai des întâlnite în rândul furnizorilor chestionaţi;

- standardele/recomandările sau alte documente/publicaţii de standardizare europene şi/sau

internaţionale utilizate de furnizori pentru implementarea unor măsuri în domeniul managementului incidentelor şi modul/gradul de utilizare a acestor documente.

Printre tipurile de incidente cel mai greu de detectat se numără:

- incidentele care nu generează alarme, performanţele 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 destinaţii cu scopul congestionării reţelei;
- incidentele care se manifestă doar prin testarea intrusivă asupra serviciului;
- incidentele referitoare la vulnerabilităţi de tip *zero-day*;
- incidentele care se manifestă intermitent;
- incidentele care se pot identifica doar la faţa locului;
- incidentele de tip *APT (Advanced Persistent Threats*);
- probleme întâmpinate în retransmisia programelor audiovizuale;
- deviaţiile de calitate în cazul serviciilor mobile (este dificil să se identifice proactiv toate zonele unde pot apărea deviaţii de la calitate datorită specificului reliefului);
- defectarea unor echipamente sau linii de transmisie care nu se pot monitoriza sau nu generează alarme;
- erorile de configuraţie care nu sunt evidente, dar care afectează buna funcţionare a echipamentelor;
- măsurarea cu acurateţe a nivelului de zgomot şi detectarea sursei;
- reclamaţiile de la clienţi care nu conţin informaţii necesare identificării cauzei.

Printre incidentele cel mai greu de remediat, se numără:

- incidentele care presupun acces fizic la locaţie;
- incidentele care implică resurse ce nu sunt sub controlul furnizorului;
- incidentele produse în locaţii izolate;
- incidentele cauzate de condiţii meteorologice nefavorabile;
- incidentele ce necesită intervenţia unor echipe suplimentare, eventual din afara organizaţiei, în vederea soluţionării;
- incidentele cauzate de distrugerea fibrei optice;
- incidentele cauzate de lipsa alimentării cu energie electrică în condiţii de calamitate sau în condiţii meteorologice nefavorabile.

6 furnizori au oferit informaţii privind problemele frecvente cu care se confruntă în ceea ce priveşte detectarea şi raportarea evenimentelor/incidentelor/vulnerabilităţilor.
Printre acestea se regăsesc lipsa automatizării, dificultatea localizării incidentului, degradarea punctuală a calităţii unui serviciu, eterogenitatea sistemelor atât din perspectiva tehnologiilor, cât şi a vendorilor care fac necesară existenţa procedurilor dependente de echipamente pentru detectarea aceluiaşi tip de incident, lipsa unui domeniu actualizat în care să se regăsească metode şi proceduri de detectare a posibilelor vulnerabilităţi/incidente.

4 furnizori au oferit informaţii privind problemele frecvente cu care se confruntă în ceea ce priveşte analiza, evaluarea, trierea incidentelor. Necesitatea stabilirii impactului înainte de analiza detaliată a incidentului sau probleme legate de resursele umane implicate sunt exemple menţionate de furnizori în acest sens.

În ceea ce priveşte răspunsul la incidente, inclusiv escaladarea, 8 furnizori au oferit informaţii referitoare la problemele cu care se confruntă. Printre problemele prezentate, se numără:

- necesitatea estimării unui termen de remediere înainte de a avea informaţii de la faţa locului (pentru incidente care necesită intervenţie în teren în vederea soluţionării);

- aspecte legate de resursele umane implicate;

- întârzieri în procesul de răspuns prin faptul că prima echipă selectată automat nu este abilitată să rezolve problema direct;

- reveniri şi escaladări administrative pentru a face ca răspunsurile/cauza să fie comunicate;

- dependenţa de terţi/alţi furnizori care oferă infrastructură;

- dificultăţi legate de realizarea sincronizării tuturor participanţilor la incidentele produse (de exemplu trebuie convocate şi echipe din afara organizaţiei).

3 furnizori au menţionat problemele cu care se confruntă în privinţa colectării informaţiilor despre incidente şi păstrării evidenţei acestora. Acestea se referă la insuficienţa informaţiilor pentru urmărirea facilă a istoricului incidentelor, decelarea între evenimentele existente în reţea ca status normal şi cele care pot conduce la incidente în cazul netratării proactive, resursele umane implicate.

Referitor la comunicarea informaţiilor despre incidente unor părţi externe, 4 furnizori au precizat problemele pe care le întâmpină: lipsa de contacte, inexistenţa unui model standard pentru comunicare, lipsa de reactivitate la solicitările organizaţiei.

Furnizorilor li s-a cerut să prezinte particularităţile tipului de incident cel mai des întâlnit (având caracteristici similare altor incidente în ceea ce priveşte cauza producerii incidentului, resursele afectate sau alte considerente ce pot încadra mai multe incidente într-o anumită tipologie) în cadrul propriilor organizaţii pe parcursul anului 2014.

Răspunsurile primite au scos în evidenţă cauza cel mai des întâlnită a incidentelor şi anume probleme privind alimentarea cu energie electrică, 8 furnizori menţionând incidentele provocate de această cauză ca fiind cel mai des întâlnite tipuri de incidente. Alţi 4 furnizori au menţionat incidentele legate de secţionări/ruperi accidentale/distrugeri şi/sau furturi ale cablurilor (subterane sau aeriene, de cupru sau de fibră optică) ca fiind cele mai frecvente incidente înregistrate pe parcursul anului 2014. Alte incidente des întâlnite au fost cele cauzate de condiţii meteorologice nefavorabile, atacuri de tip *DDoS*, atacuri cibernetice asupra unor sisteme de calcul.

Furnizorii au fost rugaţi să menţioneze standardele/recomandările sau alte documente/publicaţii de standardizare europene şi/sau internaţionale utilizate de propriile organizaţii pentru implementarea unor măsuri în domeniul managementului incidentelor, specificând şi modul/gradul de utilizare (de exemplu parţial, total, adaptat) a acestor documente.

13 respondenţi (3 furnizori nu au răspuns) au menţionat standardul *ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements*. Dintre aceştia, 7 furnizori au menţionat şi alte documente de referinţă precum *ISO27002:2005 Information technology - Security techniques - Code of practice for information security management, ISO 9001 Quality management systems - Requirements, ISO 14001 Environmental management systems - Requirements with guidance for use*, *BS OHSAS 18001 Occupational Health and Safety Management*, *ISO 22301 Societal security - Business continuity management systems - Requirements*, standarde *NIST* (*National Institute of Standards and Technology*), ghiduri *ISACA* (*Information Systems Audit and Control Association*), ghiduri *ENISA* (*European Union Agency for Network and Information Security*), standarde şi recomandări *eTOM*, *ITIL*. Nu au fost oferite informaţii relevante privind modul/gradul de utilizare a documentelor menţionate.

V. Concluzii

Prezentul raport tratează managementul incidentelor din perspectiva măsurilor de securitate pe care furnizorii trebuie să le implementeze în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, conform obligaţiilor legale: stabilirea de procese şi proceduri pentru managementul incidentelor, sisteme de detectare a incidentelor, proceduri şi planuri de comunicare a incidentelor.

Raportul reflectă abordările şi practicile celor 16 furnizori chestionaţi în ceea ce priveşte managementul incidentelor. Prin intermediul acestuia, ANCOM îşi propune să sprijine furnizorii chestionaţi prin diseminarea informaţiilor referitoare la bunele practici existente în domeniul managementului incidentelor, aşa cum rezultă din răspunsurile oferite la chestionar.

Răspunsurile la Chestionarul privind implementarea măsurilor de securitate în domeniul managementului incidentelor au scos în evidenţă faptul că în rândul furnizorilor chestionaţi există o preocupare activă în ceea ce priveşte managementul incidentelor.

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

1. În rândul furnizorilor chestionaţi există diverse abordări în ceea ce priveşte documentaţia aferentă managementului incidentelor şi mai multe tipuri de documente/modalităţi de prezentare a proceselor, rolurilor şi responsabilităţilor asociate managementului incidentelor, alese în funcţie de normele interne ale organizaţiei.

2. Referitor la compartimentul/echipa dedicată activităţilor de management al incidentelor, există mai multe situaţii: unii furnizori au un compartiment/departament dedicat acestor activităţi, cu o echipă de răspuns la incidente în cadrul propriilor organizaţii, alţii au persoane desemnate care să se ocupe de managementul/tratarea incidentelor, alţi furnizori au un contract de prestări servicii în acest sens/aceste servicii sunt externalizate, dar în cazul lor există şi structuri interne dedicate activităţilor de tratare a incidentelor.

3. Printre tipurile de incidente menţionate de furnizori care intră în aria de competenţă/activitate a compartimentului de tratare a incidentelor/echipei de răspuns la incidente se află acele evenimente care pot afecta resursele, procesele sau obiectivele organizaţiei, incidente ce afectează funcţionarea reţelelor şi serviciilor de comunicaţii electronice, incidente de securitate cibernetică.

4. Răspunsurile la chestionar au indicat că furnizorii deţin 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/vulnerabilităţi.

5. Toţi furnizorii chestionaţi au afirmat că au o evidenţă a incidentelor petrecute în cadrul propriilor organizaţii.

6. În majoritatea cazurilor, procedurile privind managementul incidentelor acoperă procesele de detectare şi raportare internă, evaluare/triere şi decizie, răspuns, escaladare, colectare a informaţiilor despre incidente şi păstrarea evidenţei acestora. Procedurile privind managementul incidentelor cuprind şi definirea, respectiv alocarea rolurilor şi responsabilităţilor persoanelor adecvate.

7. Toţi furnizorii deţin metode/instrumente/mecanisme pentru determinarea/măsurarea şi monitorizarea tipului incidentelor petrecute.

8. Cea mai frecventă cauză a incidentelor este reprezentată de problemele referitoare la alimentarea cu energie electrică.

9. În cazul incidentelor, cel mai frecvent afectate categorii de resurse sunt echipamente auxiliare (de alimentare/de backup cu energie electrică, sisteme de răcire etc.), routere şi switch-uri IP, cabluri (terestre, aeriene sau subterane).

10. Cei mai mulţi furnizori organizează întâlniri ad-hoc, în urma incidentelor majore, între membrii echipei de răspuns/personalul responsabil cu managementul/tratarea incidentelor, în care se analizează incidentul respectiv.

11. Majoritatea furnizorilor au sisteme/instrumente atât pentru detectarea proactivă, cât şi pentru detectarea reactivă a evenimentelor/incidentelor.

12. Evenimentele/incidentele ce pot afecta/afectează furnizarea reţelelor şi serviciilor de comunicaţii electronice pot fi detectate prin instrumente/sisteme automate şi pe baza unor sesizări/informări din partea personalului organizaţiei, din partea unor părţi externe precum organizaţii de profil/parteneri de afaceri, alţi furnizori de reţele şi servicii de comunicaţii electronice, precum şi din partea utilizatorilor de reţele şi servicii de comunicaţii electronice.

13. Monitorizarea reţelei de comunicaţii electronice se realizează atât la nivel de reţea/serviciu, la nivel de echipamente distincte, cât şi la nivel de aplicaţii distincte. Soluţiile/sistemele/aplicaţiile utilizate de furnizorii respondenţi pentru monitorizarea elementelor/echipamentelor reţelei de comunicaţii electronice se referă în principiu la sisteme de management/monitorizare de tip *OSS*, *NMS*.

14. Furnizorii chestionaţi monitorizează şi reţeaua internă a organizaţiei.

15. În ceea ce priveşte procedurile şi planurile de comunicare a informaţiilor despre incidente, furnizorii deţin un proces privind comunicarea informaţiilor despre incidente unor părţi externe. Procesul de comunicare este susţinut de proceduri şi/sau planuri de comunicare a informaţiilor despre incidente pentru mulţi dintre furnizori, majoritatea furnizorilor chestionaţi au un proces de raportare a incidentelor către ANCOM, însă un număr restrâns deţine proceduri specifice în care este detaliat acest proces.

16. De regulă utilizatorilor le sunt comunicate incidentele majore/critice.

17. Printre mijloacele/instrumentele cel mai des utilizate de furnizori pentru comunicarea informaţiilor despre incidente utilizatorilor de reţele şi servicii de comunicaţii electronice se regăsesc *call center*-ul, *IVR*-ul, e-mailul, SMS-ul.

18. Cei mai mulţi furnizori comunică diverselor părţi externe unele informaţii despre incidente nestandardizat, prin metode alese în funcţie de circumstanţele incidentului (comunicare ad-hoc).

19. Dintre documentele de standardizare europene şi/sau internaţionale utilizate pentru implementarea unor măsuri în domeniul managementului incidentelor, majoritatea furnizorilor au menţionat standardul *ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements*.

Având în vedere potenţialul impact al incidentelor asupra propriei organizaţii şi asupra utilizatorilor finali, furnizorii trebuie să accentueze importanţa oferită managementului incidentelor.

Implementarea unor măsuri corespunzătoare pentru protecţia reţelelor şi serviciilor de comunicaţii electronice, acoperind resurse hardware, software (echipamente de reţea, sisteme, aplicaţii etc.) şi alte tipuri de resurse ce pot fi implicate în procesul furnizării reţelelor şi serviciilor de comunicaţii electronice trebuie să conducă la reducerea frecvenţei de apariţie a incidentelor în cadrul organizaţiei. Prevenirea incidentelor este de regulă mult mai eficientă şi mai puţin costisitoare decât răspunsul/reacţia la acestea. Astfel, se recomandă ca organizaţia să-şi orienteze activităţile de tratare a incidentelor nu numai spre acţiuni reactive, ci şi spre eforturi proactive.

ANCOM are în vedere şi elaborarea unui Ghid de implementare a măsurilor de securitate în domeniul managementului incidentelor conform prevederilor Deciziei nr.512/2013. Ghidul se va adresa tuturor furnizorilor de reţele şi servicii de comunicaţii electronice şi va oferi îndrumări/recomandări pentru implementarea anumitor măsuri în acest domeniu.

VI. Anexă

Lista furnizorilor către care s-a transmis chestionarul

Nr.	Furnizor
1	DIGITAL CABLE SYSTEMS S.A.
2	EUROWEB ROMANIA S.A.
3	FOCUS SAT ROMANIA S.R.L.
4	GTS TELECOM S.R.L.
5	NEXTGEN COMMUNICATIONS S.R.L.
6	ORANGE ROMÂNIA S.A.
7	PRIME TELECOM S.R.L.
8	RCS & RDS S.A.
9	SOCIETATEA COMERCIALĂ PENTRU SERVICII DE TELECOMUNICAŢII ŞI TEHNOLOGIA INFORMAŢIEI ÎN REŢELE ELECTRICE DE TRANSPORT \"TELETRANS\" S.A.
10	SOCIETATEA NAŢIONALĂ DE RADIOCOMUNICAŢII S.A.
11	TELECOMUNICAŢII C.F.R. S.A.
12	TELEKOM ROMANIA COMMUNICATIONS S.A. (FOSTA ROMTELECOM S.A.)
13	TELEKOM ROMANIA MOBILE COMMUNICATIONS S.A. (FOSTA COSMOTE ROMANIAN MOBILE TELECOMMUNICATIONS S.A.)
14	TELEMOBIL S.A.
15	UPC ROMANIA S.R.L.
16	VODAFONE ROMANIA S.A.