ANCOM
Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii

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

Raport
privind măsurile implementate de furnizori pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice

Prin planul de acţiuni pe anul 2012, ANCOM şi-a propus stabilirea măsurilor minime de securitate ce trebuie implementate de către furnizorii de reţele şi servicii de comunicaţii electronice. Astfel, în vederea analizării/estimării nivelului de securitate şi integritate al reţelelor şi serviciilor de comunicaţii electronice existent la momentul actual şi identificării măsurilor ce sunt deja implementate, în luna iulie 2012, ANCOM a transmis către 20 de furnizori de reţele şi servicii de comunicaţii electronice un chestionar[1] privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice. Cei 20 de furnizori deţineau la 31.12.2011 peste 90% din cota de piaţă a serviciilor de comunicaţii electronice la nivel naţional. Chestionarul a cuprins 43 de întrebări structurate în 7 mari teme: aspecte generale privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, managementul riscului, măsuri privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, monitorizarea incidentelor, informarea utilizatorilor cu privire la incidentele semnificative, testarea şi evaluarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, costul şi beneficiile măsurilor de securitate.

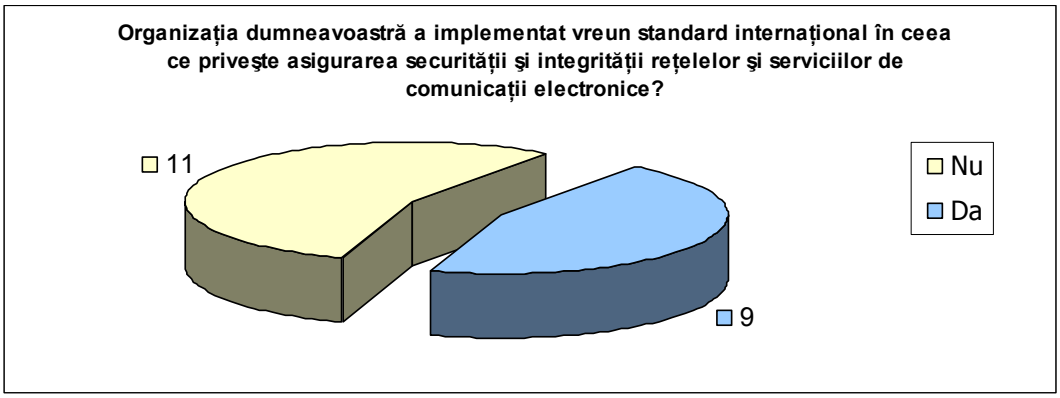
În înţelesul acestui chestionar, securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice s-a definit ca fiind capacitatea unei reţele sau a unui serviciu de comunicaţii electronice de a rezista evenimentelor accidentale, ilicite sau rău intenţionate, care pot compromite/afecta continuitatea furnizării reţelelor şi serviciilor, la un nivel de performanţă echivalent cu cel anterior producerii evenimentului.

În urma centralizării şi analizei răspunsurilor la chestionare, au fost identificate următoarele aspecte:

I. Aspecte generale privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice

În ceea ce priveşte asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, ANCOM a fost interesată, prin intermediul acestui chestionar, de măsura în care sunt utilizate standardele internaţionale în domeniu. Astfel, conform răspunsurilor primite, 9 dintre furnizorii chestionaţi au afirmat că folosesc/au implementate astfel de standarde.

[1] Chestionarul transmis furnizorilor este cuprins în Anexa la prezentul raport.

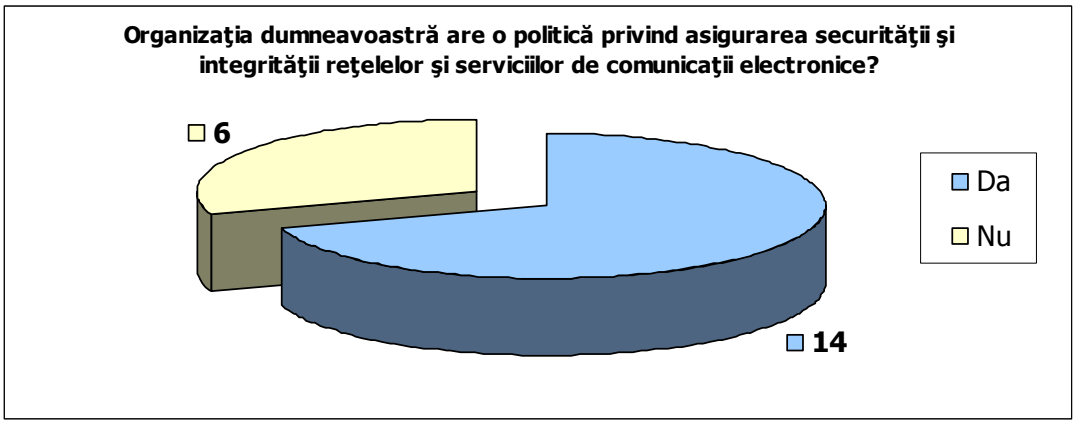


Sursa: ANCOM, pe baza răspunsurilor primite

Cel mai frecvent implementat standard internaţional în ceea ce priveşte asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice în rândul organizaţiilor furnizorilor de reţele şi servicii de comunicaţii electronice este *ISO/CEI 27001 (Information Technology – Security techniques - Information security management systems - Requirements)*, standard internaţional care a fost elaborat pentru a furniza un model pentru stabilirea, implementarea, funcţionarea, monitorizarea, revizuirea, întreţinerea şi îmbunătăţirea unui Sistem de Management pentru Securitatea Informaţiei (SMSI), SMSI conceput astfel încât să asigure selectarea adecvată şi proporţională a măsurilor de securitate care protejează resursele informatice şi încrederea părţilor implicate. Un alt standard menţionat de furnizori este BSI BS25999-1 - Guide to Business Continuity Management. Patru furnizori dintre cei chestionaţi au afirmat că sunt certificaţi *ISO/CEI 27001.*

Conform răspunsurilor primite, alegerea standardelor internaţionale (de regulă *ISO/CEI 27001*) se bazează pe motive precum: notorietatea internaţională recunoscută, recomandarea auditorilor, necesitatea de a oferi clienţilor garanţia unor servicii ce asigură disponibilitatea, confidenţialitatea şi integritatea comunicaţiilor, menţinerea unui echilibru între costuri şi beneficii, impunerea de către directivele şi recomandările internaţionale, naţionale şi de procedurile interne, nevoia de consolidare a calităţii serviciilor de comunicaţii electronice oferite, protecţia şi siguranţa fizică şi informatică a reţelelor şi a datelor cu caracter personal, deţinerea unui control organizat şi reglementat asupra protejării informaţiilor şi a resurselor asociate împotriva utilizării, modificării, divulgării sau distrugerii neautorizate – accidentale sau intenţionate, încrederea conferită clienţilor, angajaţilor, partenerilor contractuali în privinţa securităţii informaţiilor şi a sistemelor informatice etc.

În ceea ce priveşte politica privind asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, 14 furnizori au declarat că deţin o astfel de politică. Se remarcă o diferenţă considerabilă între numărul furnizorilor ce au implementat standarde internaţionale în domeniul securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice (9) şi numărul celor ce deţin o politică privind asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice (14). Astfel, cu toate că nu toţi furnizorii folosesc un standard internaţional, aceştia manifestă angajament pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor prin deţinerea unor politici adecvate.

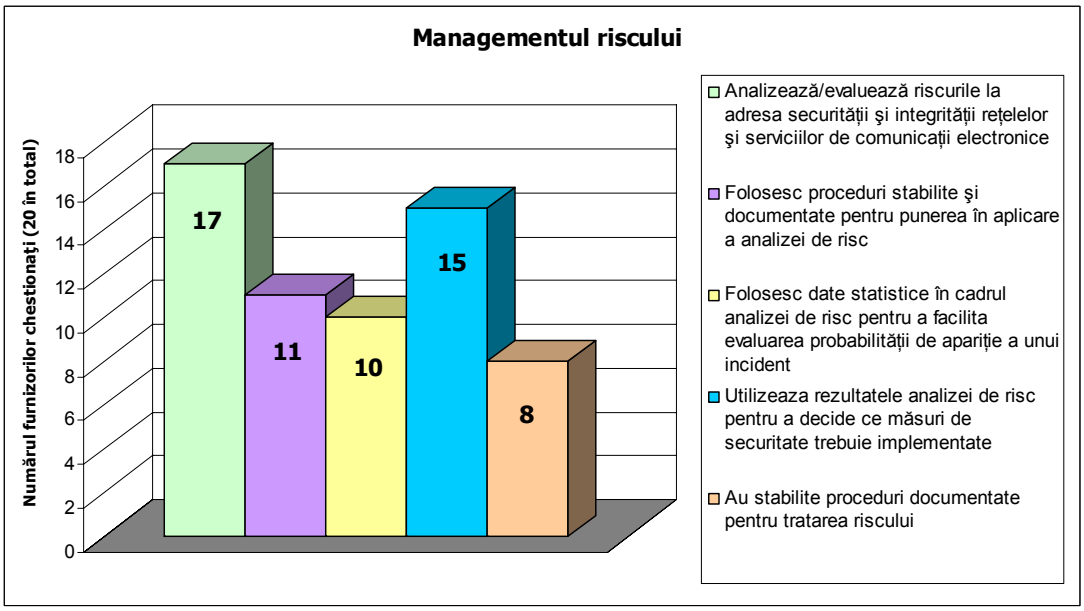


Sursa: ANCOM, pe baza răspunsurilor primite

Referitor la elementele cuprinse în politica privind asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, se remarcă faptul că există foarte puţine elemente comune în rândul respondenţilor. În plus, se constată că există neclarităţi în ceea ce priveşte scopul şi obiectivele documentului de politică, procedurilor operaţionale şi măsurilor de securitate. Astfel, elementele cuprinse în politicile furnizorilor sunt: obiective de securitatea informaţiei şi integrarea lor în procesele sistemului de management al securităţii informaţiei, principii privind asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei, managementul riscurilor, instruirea şi conştientizarea personalului cu privire la necesitatea îndeplinirii responsabilităţilor aferente securităţii informaţiei, atribuirea de roluri şi responsabilităţi specifice pentru securitatea informaţiei în cadrul organizaţiei, protejarea disponibilităţii şi integrităţii resurselor hardware şi software utilizate de sistemele, reţelele şi aplicaţiile din cadrul organizaţiei, accesul angajaţilor la nodurile de reţea, accesul la echipamente şi accesul fizic (în centre de date etc.), monitorizarea reţelelor şi a incidentelor de securitate, securitatea resurselor umane, a mediului de lucru, stabilirea/implementarea unor planuri de continuitate şi recuperare în caz de dezastru sau crize majore.

II. Managementul riscului

În privinţa managementului riscului, răspunsurile celor 20 de furnizori de reţele şi servicii de comunicaţii electronice chestionaţi au condus la următoarele rezultate:



Sursa: ANCOM, pe baza răspunsurilor primite

17 furnizori analizează/evaluează riscurile la adresa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, doar 12 dintre aceştia însă (60% dintre cei chestionaţi) au descris procesele utilizate în cadrul analizei de risc. În rândul respondenţilor, analiza de risc este percepută în mod diferit (nu există o înţelegere uniformă a acestui concept), neexistând o delimitare clară între procesele analizei, evaluării, tratării riscurilor. Majoritatea răspunsurilor se depărtează de analiza de risc, abordând un cadru mai larg ce include aspecte aferente întregului proces de management al riscurilor (stabilirea echipei implicate în procesul de management al riscurilor, identificarea şi evaluarea riscurilor la adresa securităţii, realizarea unei analize de impact asupra afacerii, stabilirea unor măsuri în scopul tratării riscurilor, monitorizarea şi îmbunătăţirea măsurilor luate). Doar 8 furnizori identifică procese similare, ce ar putea fi incluse în cadrul analizei de risc. Printre aceste procese, se regăsesc: identificarea resurselor şi abordarea detaliată, în ordinea priorităţilor resurselor cu valoare mare sau grad de expunere ridicat, identificarea riscurilor cu care se confruntă aceste resurse ale companiei, analiza probabilităţii de apariţie a evenimentelor de securitate, analiza de impact asupra afacerii (*Bussiness Impact Analysis*) etc.
Din răspunsurile furnizorilor a reieşit că, în multe cazuri, analiza de risc este foarte sumară şi tratează puţine din aspectele pe care le-ar putea trata o analiză de risc completă şi riguroasă. Astfel, numai 11 furnizori (55% dintre cei chestionaţi) folosesc proceduri stabilite şi documentate pentru punerea în aplicare a analizei de risc.

Datele statistice din cadrul analizei de risc pot reprezenta un instrument util în evaluarea probabilităţii de apariţie a unui incident, însă doar jumătate din numărul furnizorilor chestionaţi folosesc astfel de date statistice.

12 furnizori susţin că evaluările de risc sunt actuale. Printre măsurile comune menţionate pentru actualizarea evaluărilor de risc se regăsesc revizuirile periodice (de regulă anuale) ale analizei de risc. Actualizarea analizei de risc se realizează atât periodic, cât şi în funcţie de necesităţi, în cazul producerii unor schimbări majore (exemplu: dezvoltarea unor sisteme sau schimbarea deţinătorului resursei în cauză), acolo unde se observă deviaţii de la anumite praguri operaţionale stabilite prin consens, prin indicatori de performanţă şi proceduri etc.

Şapte furnizori dintre cei chestionaţi realizează actualizări complexe ale evaluărilor de risc prin acţiuni precum: monitorizarea şi evaluarea evenimentelor din reţea şi analiza incidentelor apărute la nivel de reţea, informări externe, audituri de securitate periodice (de regulă anuale), evaluări de risc tehnic şi de afacere ale proiectelor nou lansate, testarea redresării tehnice (inclusiv într-un alt amplasament decât cel curent), realizarea unor simulări, prezentarea de exemple etc.

Se disting anumite etape ce sunt parcurse în vederea implementării managementului de risc ce are drept consecinţă eliminarea, diminuarea sau acceptarea riscului: stabilirea contextului în care se desfăşoară analiza de risc, identificarea riscurilor potenţiale, analiza probabilistică a riscurilor, evaluarea şi ierarhizarea riscurilor, concretizarea efectelor riscurilor, comunicarea/ consultarea cu părţile interesate/afectate, monitorizarea şi revizuirea sistemului de management al riscurilor. Managementul riscului cuprinde modul de identificare, măsurare, control şi minimizare a efectelor în sistemele şi reţelele de comunicaţii la un nivel proporţional cu valoarea resurselor protejate. Conform răspunsurilor primite, numărul de clienţi ce sunt/pot fi afectaţi, nivelul de satisfacţie al acestora, costurile implicate, probabilitatea apariţiei incidentelor sunt factori importanţi pe baza cărora se decide asupra opţiunilor de tratare a riscurilor.

Măsurile de securitate adecvate trebuie decise/selectate în urma unui proces complet de evaluare a riscurilor. 15 furnizori (75% dintre cei chestionaţi) utilizează rezultatele analizei de risc pentru a decide ce măsuri de securitate trebuie implementate.

Tratarea riscurilor este realizată în mod diferit de către organizaţiile furnizorilor respondenţi, doar 2 dintre aceştia prezintă detaliat metodologia proprie pe baza căreia se decide asupra opţiunilor de tratare a riscurilor, inclusiv metoda de calcul care presupune evaluarea unei matrice a riscurilor. Astfel, conform acestor descrieri ale metodologiilor, riscul brut (evaluat înainte ca orice acţiune să fie luată pentru a-l trata) şi cel rezidual (rămas după tratarea riscului brut) sunt factori importanţi ai acestui proces de tratare a riscurilor, iar nivelul de risc este evaluat în funcţie de impactul financiar/operaţional/asupra reputaţiei (exemplu: nesemnificativ, minor, mediu, major, extrem) şi de probabilitatea ca riscul să aibă loc (exemplu: sigur, foarte probabil, posibil, puţin probabil, rar). Decizia ca riscurile să fie eliminate, diminuate sau acceptate este luată în funcţie de

nivelul de risc estimat. Numai 8 furnizori (40% dintre cei chestionaţi) au declarat că au stabilite proceduri documentate pentru tratarea riscului.

III. Măsuri privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice

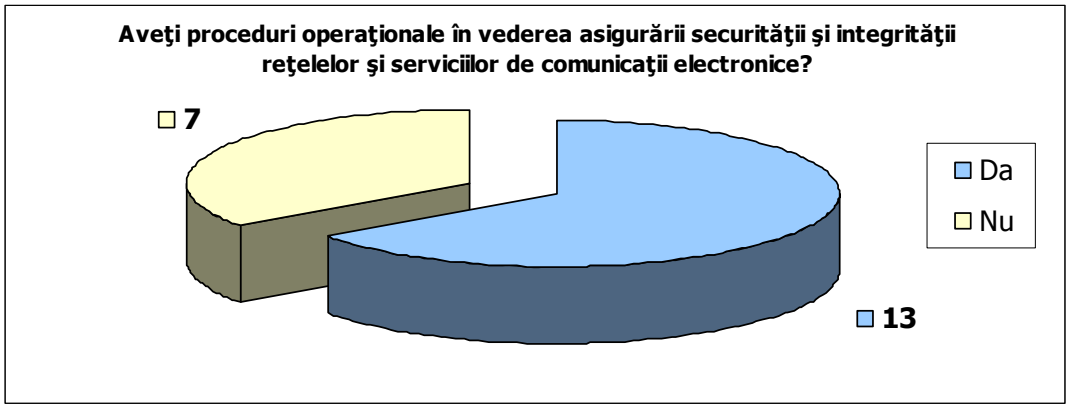
95% dintre furnizorii chestionaţi au afirmat că au implementate măsuri privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

Conform răspunsurilor primite, principalele criterii pe baza cărora se stabilesc aceste măsuri sunt reprezentate de necesitatea asigurării disponibilităţii, confidenţialităţii şi integrităţii comunicaţiilor (la nivel fizic şi logic) prin protejarea fizică a resurselor/echipamentelor, limitarea accesului logic la echipamente, protejarea resurselor critice, asigurarea redundanţei, mentenanţei, acordarea drepturilor în funcţie de rolul angajaţilor în organizaţii. Totodată, măsurile de securitate sunt luate pe baza evoluţiei numărului de clienţi, a apariţiei de noi incidente care necesită luarea măsurilor de securitate adecvate, a gradului de risc şi vulnerabilitate a resurselor, a analizării avantajelor şi beneficiilor ce pot rezulta în urma implementării acestor măsuri şi a bugetului disponibil.

Printre obiectivele implementării măsurilor privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, se regăsesc: reducerea semnificativă a numărului de incidente/întreruperi operaţionale şi a riscului de apariţie al acestora, asigurarea securităţii informaţiilor, maximizarea disponibilităţii şi a calităţii serviciilor oferite, creşterea numărului de clienţi, îmbunătăţirea proceselor operaţionale, securizarea afacerii, evitarea folosirii în mod abuziv a resurselor, protejarea confidenţialităţii datelor clienţilor şi ale companiei. Alte obiective menţionate sunt: reducerea fraudelor, prejudiciilor ce pot fi aduse companiilor/partenerilor de afaceri/clienţilor, asigurarea integrităţii fizice a locaţiilor şi a echipamentelor, asigurarea redundanţei, îmbunătăţirea gradului de conştientizare şi de răspuns operativ la incidente, creşterea încrederii în viitorul tehnologic şi comercial al companiei, asigurarea orientării generale de management pentru securitatea reţelelor de comunicaţii electronice în conformitate cu cerinţele de afacere şi legislaţia aplicabilă, asigurarea stabilirii şi asumării responsabilităţii pentru protecţia corespunzătoare a resurselor, prevenirea pierderii, distrugerii, furtului sau compromiterii sistemelor componente ale reţelelor de comunicaţii electronice, reducerea riscurilor aferente implementării noilor sisteme şi modificărilor în sistemele existente, asigurarea controlului corespunzător al accesului la resursele organizaţiei etc.

18 furnizori (90% dintre cei chestionaţi) au afirmat că, în cadrul propriilor organizaţii, sunt stabilite rolurile şi responsabilităţile în asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, iar angajaţii organizaţiei au cunoştinţe suficiente de securitate şi sunt instruiţi cu privire la securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

În cazul deţinerii unor proceduri operaţionale în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, 13 furnizori au menţionat că deţin astfel de proceduri.



Sursa: ANCOM, pe baza răspunsurilor primite

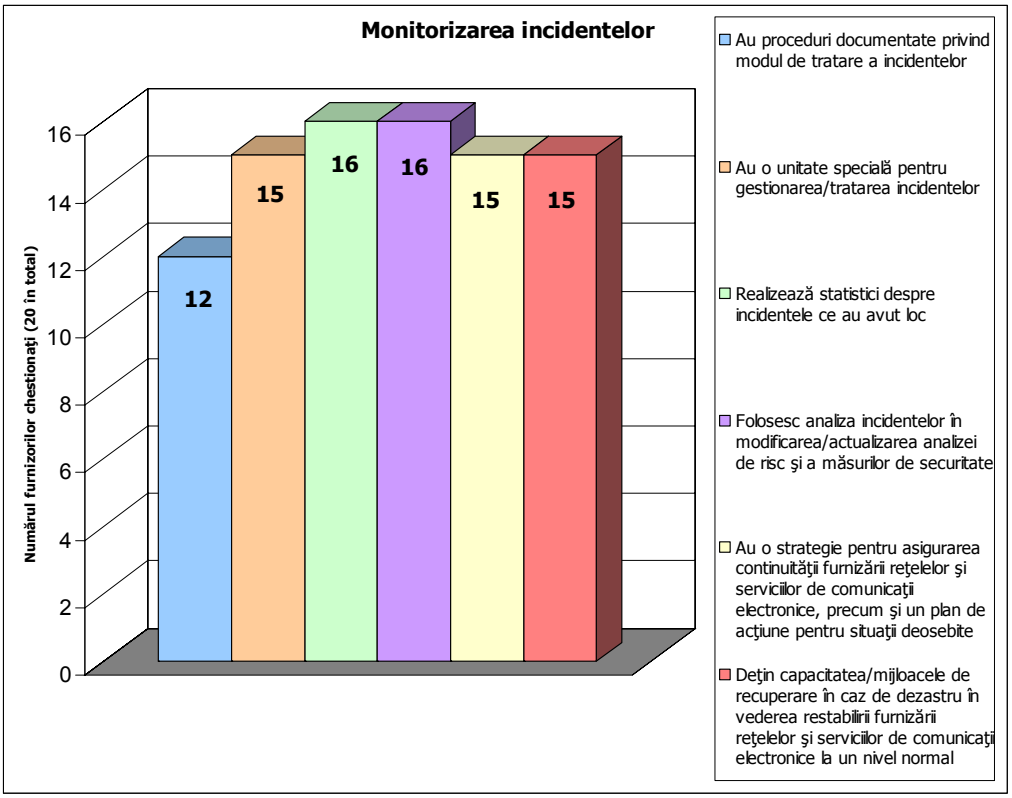
Printre domeniile tratate de aceste proceduri, se regăsesc: organizarea securităţii informaţiei (exemplu: procedura privind clasificarea informaţiilor), accesul la reţelele şi serviciile de comunicaţii electronice (exemplu: procedura de acces fizic, procedura de acces al terţilor la reţea), managementul resurselor, al operaţiunilor, al incidentelor, relaţiile cu terţii, managementul schimbărilor în sistemele informatice, administrarea utilizatorilor, securitatea resurselor umane. Sunt foarte puţine cazurile în care se menţionează şi alte domenii precum: continuitatea afacerii, planuri de urgenţă şi soluţii de recuperare în caz de dezastru pentru sistemele ce susţin reţelele şi serviciile de comunicaţii electronice, proiectare şi planuri de arhitectură, testarea software-ului.

Majoritatea furnizorilor chestionaţi (90% dintre aceştia) au afirmat că au, de asemenea, proceduri privind managementul schimbărilor efectuate în reţeaua de comunicaţii electronice şi în software-urile de aplicaţii, iar înainte de realizarea acestor schimbări sunt efectuate teste.

85% dintre furnizorii chestionaţi au descris măsurile de asigurare a redundanţei utilizate pentru resursele/funcţiile critice din cadrul propriilor organizaţii. Multe răspunsuri au inclus măsuri precum: utilizarea dispozitivelor UPS şi a generatoarelor electrice care să asigure funcţionarea neîntreruptă a echipamentelor în cazul opririi alimentării curentului electric de la reţeaua principală, asigurarea echipamentelor de *back-up* (rezervă/copii de siguranţă) pentru resursele critice, capacităţi de rezervă pentru elementele de reţea şi căi redundante pentru elementele de transport. Un număr redus de respondenţi au inclus măsuri de asigurare a redundanţei precum: sisteme active redundante, soluţii de back-up şi recuperare în caz de dezastru (*disaster recovery*) pentru funcţiile critice şi continuitatea afacerii, redundanţa legăturilor de reţea prin care se furnizează accesul la serviciile oferite de organizaţie clienţilor săi, redundanţă geografică pentru echipamente pentru a rezista în caz de dezastru, utilizarea protocoalelor de rutare dinamică şi de reconfigurare automată, rutări alternative, efectuarea de back-up periodic al tuturor informaţiilor din centre de date şi stocarea acestora în spaţii aflate la anumite distanţe de cele principale cu asigurarea unor condiţii similare de securitate, asigurarea unor linii dedicate de back-up pentru comunicaţiile vitale.

IV. Monitorizarea incidentelor

Pe baza răspunsurilor primite, situaţia privind monitorizarea incidentelor de securitate în rândul furnizorilor de reţele şi servicii de comunicaţii electronice chestionaţi se prezintă astfel:



Sursa: ANCOM, pe baza răspunsurilor primite

Se remarcă faptul că mulţi furnizori folosesc analiza incidentelor pentru modificarea/actualizarea măsurilor de securitate, dar unii exclud analiza de risc din demersul lor.

11 furnizori (55% dintre cei chestionaţi) au oferit informaţii referitoare la frecvenţa de testare a procedurilor şi planurilor de acţiune privind modul de tratare a incidentelor.

Testarea acestor proceduri (aşa cum reiese din răspunsurile primite) se realizează periodic, cel puţin anual. Puţine organizaţii testează aceste proceduri în funcţie de necesităţi, atunci când apar schimbări în domeniul de activitate, în procese sau atunci când sunt semnalate incidente semnificative.

18 furnizori (90% dintre cei chestionaţi) au descris modul de monitorizare a incidentelor de securitate. Jumătate dintre aceştia au detaliat modalităţile folosite, reuşind să ofere o imagine asupra monitorizării incidentelor în propriile organizaţii, accentul fiind pus pe monitorizarea incidentelor apărute în reţea. Conform acestora, monitorizarea incidentelor din reţea se realizează permanent (24 de ore din 24), în timp real, prin folosirea unor sisteme automate/softuri specializate de monitorizare care centralizează toate alarmele generate de echipamente şi oferă posibilitatea filtrării, corelării, verificării şi validării alarmelor primite. Înregistrarea incidentelor, păstrarea jurnalelor de audit în care sunt înregistrate activităţile reţelei şi cele ale sistemelor de procesare a informaţiei sunt aspecte menţionate mai rar de către respondenţi.

Majoritatea furnizorilor chestionaţi au afirmat că, în cadrul propriilor organizaţii, personalul este instruit pentru gestionarea/tratarea incidentelor.

19 furnizori (95% dintre cei chestionaţi) au descris modul de tratare a incidentelor de securitate, 6 dintre aceştia însă au descris foarte succint ori s-au depărtat de subiectul propus. Cu toate acestea, doar 12 furnizori (60% dintre cei chestionaţi) au declarat că au proceduri documentate privind modul de tratare a incidentelor. Doar în cadrul anumitor organizaţii există structuri şi sunt definite praguri de escaladare a incidentelor, iar deciziile de remediere a acestor incidente sunt luate de către echipa dedicată în funcţie de tipul, gravitatea acestora, fiind aplicate măsuri în baza metodologiilor interne de lucru. În cazul incidentelor din reţea, în urma identificării unui incident pe baza alarmelor generate de echipamentele de telecomunicaţii, se deschide un tichet într-o aplicaţie internă, se efectuează diagnoza incidentului şi, dacă este cazul, o echipă de intervenţie este trimisă pe teren. În urma soluţionării incidentului respectiv, se închide tichetul aferent. Înregistrarea incidentelor, întocmirea unor rapoarte privind incidentele identificate, stocarea unui istoric în format electronic al rezolvării fiecărui incident sunt acţiuni menţionate doar de o mică parte a furnizorilor de reţele şi servicii de comunicaţii electronice chestionaţi.

15 respondenţi au afirmat că deţin o unitate specială pentru gestionarea/tratarea incidentelor. În privinţa statisticilor referitoare la incidente, 16 furnizori (80% dintre cei chestionaţi) realizează statistici privind incidentele ce au avut loc.

15 furnizori (75% dintre cei chestionaţi) au afirmat că au o strategie pentru asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice, precum şi un plan de acţiune pentru situaţii deosebite şi tot atâţia deţin capacitatea/mijloacele de recuperare în caz de dezastru în vederea restabilirii furnizării reţelelor şi serviciilor de comunicaţii electronice la un nivel normal.

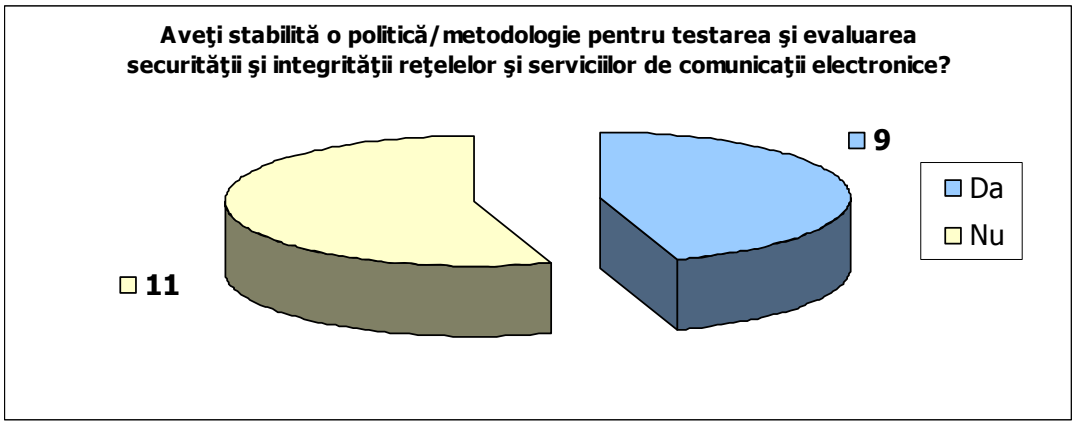
V. Informarea utilizatorilor

În privinţa informării utilizatorilor despre incidentele semnificative care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice, majoritatea furnizorilor respondenţi au declarat că oferă astfel de informaţii utilizatorilor în măsura solicitărilor sau reclamaţiilor primite. 2 furnizori aduc detalii privind desfăşurarea (în ultimele 12 luni) unor campanii doar pentru conştientizarea portofoliului de clienţi privind existenţa fraudelor sau a altor aspecte ce pot afecta securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice. În plus, 7 furnizori (dintre cei chestionaţi) au precizat că pot informa utilizatorii cu privire la incidentele semnificative (exemplu: prin mass-media), însă în ultimele 12 luni această acţiune nu s-a concretizat deoarece, în opinia furnizorilor respectivi, n-au existat incidente semnificative în intervalul temporal specificat care să afecteze securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

Printre mijloacele folosite de furnizori pentru informarea utilizatorilor, se regăsesc: telefonie, SMS, e-mail, pagina proprie de internet, scrisori de notificare/informări personalizate, centre de suport/relaţii cu clienţii (*Call Centers*), mass-media.

VI. Testarea şi evaluarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice

Stabilirea unei politici/metodologii pentru testarea şi evaluarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice este realizată de 9 furnizori (dintre cei chestionaţi):



Sursa: ANCOM, pe baza răspunsurilor primite

Doar 45% dintre furnizorii chestionaţi au descris metodologia proprie utilizată pentru testarea şi evaluarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice. O mică parte dintre aceştia au menţionat auditurile interne de securitate ca fiind elemente principale la baza cărora stă testarea securităţii, procedurile de securitate făcând parte din monitorizarea auditului intern şi fiind supuse unor planuri de testare periodice. Printre metodele de testare folosite de organizaţiile respondente, se regăsesc: teste de penetrare şi scanări periodice ale serverelor, analiza periodică/măsurători ale parametrilor de reţea, evaluarea din punct de vedere al securităţii a noilor servicii de comunicaţii electronice înainte de lansarea acestora pe piaţă, realizarea testelor de acceptanţă, realizarea unor scenarii/simulări pentru testare, testarea redresării tehnice etc.

VII. Costul şi beneficiile măsurilor de securitate

14 furnizori (70% dintre cei chestionaţi) au oferit informaţii despre costul în bani al implementării măsurilor privind securitatea şi integritatea reţelelor şi serviciilor existente. Costul este dificil de cuantizat pentru mulţi dintre respondenţi, investiţiile în securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice nefiind tratate separat, ci considerându-se ca şi parte integrantă a proiectelor mari sau a operării curente, necesare pentru dezvoltarea şi operarea reţelelor şi serviciilor de comunicaţii electronice. Pe lângă costurile aferente implementării tehnice (hardware şi software) şi a celei operaţionale, unele companii investesc în consultanţă şi documentare. Conform răspunsurilor primite, costurile depind în mare măsură de mărimea organizaţiei (ca şi număr de utilizatori, angajaţi, cifră de afaceri etc).

13 furnizori (65% dintre cei chestionaţi) aduc informaţii privind beneficiile măsurilor de securitate implementate în raport cu costul generat de implementarea lor. Printre beneficiile enumerate, se remarcă: asigurarea continuităţii serviciilor, reducerea numărului incidentelor de securitate, evitarea întreruperii activităţilor de bază ale organizaţiilor, reducerea efortului material şi uman de recuperare a datelor importante ce s-ar putea pierde în cazul incidentelor care afectează securitatea informaţiei, posibilitatea ofertării de servicii critice cu disponibilitate foarte ridicată, îmbunătăţirea calităţii serviciilor furnizate, protejarea clienţilor de eventuale atacuri informatice, creşterea încrederii în rândul clienţilor şi a partenerilor de afaceri, controlul sporit al fluxurilor de informaţii din organizaţii, asigurarea integrităţii şi disponibilităţii sistemelor şi

aplicaţiilor IT utilizate pentru operarea, livrarea şi asigurarea serviciilor companiei, reducerea costurilor de întreţinere a reţelelor, securizarea fizică a ariilor protejate, extinderea capacităţii reţelelor, promovarea afacerilor. Unii respondenţi menţionează imposibilitatea cuantificării beneficiilor enumerate, însă recunosc importanţa măsurilor de securitate implementate, considerând că efortul financiar realizat în acest scop este mai mic decât beneficiile aduse.

Dintre furnizorii chestionaţi, 12 furnizori (60% dintre cei chestionaţi) au specificat obstacolele şi dificultăţile majore întâmpinate în implementarea măsurilor privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice. Conform răspunsurilor primite, în mare parte, constrângerile se referă la partea financiară (costuri) implicată în procesul implementării măsurilor de securitate. Obstacolele intervin şi din cauza factorilor temporali sau resurselor umane implicate. De asemenea, dificultăţile întâmpinate se datorează necesităţii de aliniere continuă a măsurilor de securitate cu nevoile afacerii, necesităţii de conştientizare a clienţilor în privinţa riscurilor de securitate, limitărilor tehnice ale echipamentelor şi soluţiilor pentru asigurarea redundanţei şi securităţii accesului la echipamente etc.

În privinţa beneficiilor stabilirii unor măsuri minime de securitate şi integritate care ar trebui respectate de către furnizorii de reţele şi servicii de comunicaţii electronice, majoritatea covârşitoare a acestora recunosc necesitatea stabilirii unor astfel de măsuri în scopul asigurării continuităţii serviciilor oferite către clienţi, protejării datelor personale ale clienţilor şi angajaţilor, protejării reţelei împotriva atacurilor informatice, păstrării confidenţialităţii, integrităţii şi disponibilităţii resurselor organizaţiei, reducerii numărului incidentelor de securitate şi a reclamaţiilor la adresa securităţii, securizării afacerii, încrederii clienţilor şi măririi numărului acestora, creşterii eficienţei şi productivităţii companiilor în livrarea serviciilor către clienţi, îmbunătăţirii controlului sistemelor şi proceselor interne ale organizaţiilor, îmbunătăţirii calităţii serviciului, reducerii riscurilor în privinţa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice etc. Un singur furnizor a afirmat că aceste măsuri ar avea beneficii minime, iar altul a accentuat faptul că măsurile proprii de securitate şi integritate sunt mai exigente decât măsurile minime de securitate ce ar putea fi impuse de ANCOM, măsurile stabilite de autoritate fiind benefice (în opinia sa) pentru asigurarea unui standard minim de securitate la nivel general de industrie.

Observaţii generale/Concluzii

În urma analizării răspunsurilor primite de la cei 20 de furnizori de reţele şi servicii de comunicaţii electronice la chestionarul transmis de ANCOM, a rezultat că majoritatea dintre aceştia au o preocupare activă în asigurarea securităţii şi integrităţii reţelelor şi serviciilor. Cu toate acestea, doar o parte dintre furnizori au proceduri clare şi documentate pentru asigurarea continuităţii reţelelor şi serviciilor, în majoritatea cazurilor stabilirea unor măsuri de securitate efectuându-se reactiv, în momentul apariţiei unui incident. În plus, puţini dintre furnizori au o abordare completă a domeniului securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, majoritatea axându-se doar pe anumite domenii de interes. Prin urmare, domeniul securităţii şi integrităţii nu este abordat unitar de către furnizorii chestionaţi. Acest fapt se datorează şi inexistenţei unui standard internaţional pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor, standardul utilizat preponderent de respondenţi fiind ISO/CEI 27001, standard ce se referă în principal la securitatea informaţiei.

Majoritatea furnizorilor au indicat că deţin o politică privind asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, însă din celelalte răspunsuri nu a reieşit o direcţie clară de acţiune pe care o politică adecvată ar trebui să o impună.

Managementul riscului este un proces continuu şi trebuie să fie parte integrantă a tuturor activităţilor desfăşurate în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor. Cu toate că managementul riscurilor constituie un domeniu fundamental pe baza căruia ar trebui luată decizia stabilirii măsurilor de securitate, din răspunsurile multor furnizori a rezultat că acestui domeniu i se acordă un interes scăzut, analiza de risc nefiind completă în multe cazuri sau chiar lipsind cu desăvârşire. Astfel, rezultă că un număr relativ redus de furnizori au proceduri documentate în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice (proceduri ce includ analiza corectă, completă a riscurilor), măsurile privind securitatea

şi integritatea fiind luate de unii furnizori ad-hoc, în urma detecţiei unor probleme/apariţiei unor incidente.

Majoritatea furnizorilor chestionaţi monitorizează incidentele petrecute în reţea, însă nu toţi au proceduri în vederea tratării incidentelor, în cazul acestora acţiunile şi deciziile fiind luate în momentul apariţiei incidentului.

În ceea ce priveşte testarea securităţii şi integrităţii reţelelor şi serviciilor, o mare parte a furnizorilor nu efectuează o astfel de activitate, nefiind astfel la curent cu vulnerabilităţile existente/actuale. Din răspunsurile primite, a reieşit că doar 7 furnizori efectuează audituri de securitate pentru a se asigura că securitatea şi integritatea reţelelor este una adecvată.

În ceea ce priveşte informarea utilizatorilor cu privire la incidentele semnificative, din răspunsurile furnizorilor a reieşit că majoritatea dintre aceştia îşi informează utilizatorii doar în măsura solicitărilor acestora şi a reclamaţiilor primite, noţiunea de „incident semnificativ" fiind totodată percepută în mod diferit în rândul respondenţilor. Niciun furnizor nu şi-a informat utilizatorii din proprie iniţiativă cu privire la un incident semnificativ, principala motivaţie fiind inexistenţa vreunui incident semnificativ în ultimele 12 luni şi doar 2 furnizori au adus detalii privind desfăşurarea (în ultimele 12 luni) unor campanii pentru conştientizarea de către clienţi a existenţei fraudelor sau a altor aspecte ce pot afecta securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice.

Majoritatea furnizorilor chestionaţi au recunoscut necesitatea/beneficiile stabilirii unor măsuri minime de securitate şi integritate ce ar trebui respectate de către furnizorii de reţele şi servicii de comunicaţii electronice, printre cele mai importante beneficii regăsindu-se asigurarea continuităţii serviciilor oferite către clienţi, protejarea datelor personale ale clienţilor şi angajaţilor, păstrarea confidenţialităţii, integrităţii şi disponibilităţii resurselor organizaţiei, reducerea numărului incidentelor de securitate şi a reclamaţiilor la adresa securităţii, îmbunătăţirea controlului sistemelor şi proceselor interne ale organizaţiilor, îmbunătăţirea calităţii serviciului, reducerea riscurilor în privinţa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice.

Ca urmare a analizării răspunsurilor la chestionar, ANCOM consideră că este necesară stabilirea unor linii directoare în scopul asigurării unei securităţi şi integrităţi adecvate a reţelelor şi serviciilor. Astfel, ANCOM îşi propune - prin proiectul de decizie privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de reţele şi servicii de comunicaţii electronice şi raportarea incidentelor cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice - stabilirea domeniilor pe care trebuie să le vizeze măsurile de securitate adoptate de furnizori.

Anexă

Chestionar cu privire la securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice

În înţelesul acestui chestionar, securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice reprezintă capacitatea unei reţele sau a unui serviciu de comunicaţii electronice de a rezista evenimentelor accidentale, ilicite sau rău intenţionate, care pot compromite/afecta continuitatea furnizării reţelelor şi serviciilor, la un nivel de performanţă echivalent cu cel anterior producerii evenimentului.

Notă: în cazul în care la anumite întrebări cu răspuns deschis nu puteţi răspunde datorită faptului că nu aveţi implementate procesele respective, se va completa cu sintagma „nu este cazul".

I. Întrebări generale despre securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice

1. Organizaţia dumneavoastră a implementat vreun standard internaţional în ceea ce priveşte asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice?

☐ Da

☐ Nu

2. Menţionaţi standardele folosite de organizaţie.

3. Menţionaţi motivele pentru care aţi ales aceste standarde.

4. Organizaţia dumneavoastră are o politică privind asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice?

☐ Da

☐ Nu

5. Care sunt elementele cuprinse în această politică?

II. Analiza şi managementul riscului

6. Organizaţia dumneavoastră analizează/evaluează riscurile la adresa securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice?

☐ Da

☐ Nu

7. Folosiţi proceduri stabilite şi documentate pentru punerea în aplicare a analizei de risc?

☐ Da

☐ Nu

8. Folosiţi date statistice în cadrul analizei de risc pentru a facilita evaluarea probabilităţii de apariţie a unui incident?

☐ Da

☐ Nu

9. Descrieţi procesele utilizate în cadrul analizei de risc.

10. Descrieţi măsurile luate pentru a vă asigura că evaluările de risc sunt actuale (exemplu: factorii care determină înnoirea analizei de risc).

11. Utilizaţi rezultatele analizei de risc pentru a decide ce măsuri de securitate trebuie implementate?

☐ Da

☐ Nu

12. Aveţi stabilite proceduri documentate pentru tratarea riscului?

☐ Da

☐ Nu

13. Descrieţi criteriile pe baza cărora se decide ca riscurile să fie eliminate, diminuate sau acceptate.

III. Măsuri privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice

14. Aveţi astfel de măsuri implementate în organizaţie?

☐ Da

☐ Nu

15. Descrieţi principalele criterii pe baza cărora se stabilesc aceste măsuri.

16. Care este obiectivul implementării acestor măsuri?

17. Sunt stabilite rolurile şi responsabilităţile în asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice?

☐ Da

☐ Nu

18. Angajaţii organizaţiei au cunoştinţe suficiente de securitate şi sunt instruiţi cu privire la securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice?

☐ Da

☐ Nu

19. Aveţi proceduri operaţionale în vederea asigurării securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice?

☐ Da

☐ Nu

20. Care sunt domeniile tratate de aceste proceduri?

21. Aveţi proceduri privind managementul schimbărilor efectuate în reţeaua de comunicaţii electronice şi în software-urile de aplicaţii?

☐ Da

☐ Nu

22. Sunt efectuate teste înainte de realizarea acestor schimbări?

☐ Da

☐ Nu

23. Există redundanţă pentru resursele/funcţiile critice în asigurarea furnizării reţelelor şi serviciilor de comunicaţii electronice?

☐ Da

☐ Nu

24. Descrieţi măsurile de asigurare a redundanţei utilizate pentru resursele/funcţiile critice.

IV. Monitorizarea incidentelor

25. Aveţi proceduri documentate privind modul de raportare şi tratare a incidentelor?

☐ Da

☐ Nu

26. Cât de frecvent testaţi aceste proceduri şi planuri de acţiune?

27. Există o unitate specială pentru gestionarea/tratarea incidentelor?

☐ Da

☐ Nu

28. Descrieţi modul de monitorizare a incidentelor.

29. Personalul este instruit pentru gestionarea/tratarea incidentelor?

☐ Da

☐ Nu

30. Descrieţi modul de tratare a incidentelor (inclusiv periodicitatea monitorizării).

31. Realizaţi statistici despre incidentele ce au avut loc?

☐ Da

☐ Nu

32. Folosiţi analiza incidentelor în modificarea/actualizarea analizei de risc şi a măsurilor de securitate?

☐ Da

☐ Nu

33. Aveţi o strategie pentru asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice, precum şi un plan de acţiune pentru situaţii deosebite?

☐ Da

☐ Nu

34. Deţineţi capacitatea/mijloacele de recuperare în caz de dezastru în vederea restabilirii furnizării reţelelor şi serviciilor de comunicaţii electronice la un nivel normal?

☐ Da

☐ Nu

V. Informarea utilizatorilor

35. Informaţi utilizatorii cu privire la incidentele semnificative care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice?

☐ Da

☐ Nu

36. De câte ori au fost informaţi utilizatorii cu privire la incidentele semnificative care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice în ultimele 12 luni?

37. Prin ce mijloace au fost informaţi utilizatorii cu privire la incidentele semnificative care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice?

VI. Testarea şi evaluarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice

38. Aveţi stabilită o politică/metodologie pentru testarea şi evaluarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice?

☐ Da

☐ Nu

39. Descrieţi metodologia pentru testarea şi evaluarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice.

VII. Costul şi beneficiile măsurilor de securitate

40. Care este costul în bani al implementării măsurilor privind securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice pentru organizaţia dumneavoastră?

41. Care au fost beneficiile acestor măsuri în raport cu costul generat de implementarea lor?

42. Care au fost obstacolele şi dificultăţile majore pe care le-aţi întâmpinat în implementarea acestor măsuri?

43. În opinia dumneavoastră, care sunt beneficiile stabilirii unor măsuri de securitate şi integritate minime care ar trebui respectate de furnizorii de reţele şi servicii de comunicaţii electronice?