aprilie 2016

ANCOM
Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii

Ghid de implementare a măsurilor de securitate în domeniul managementului incidentelor conform deciziei nr.512/2013

Cuprins

Introducere

Decizia nr. 512/2013[1] stabilește în sarcina furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului obligația implementării unor măsuri de securitate (mijloace de natură administrativă, managerială, tehnică sau juridică de management al riscurilor, incluzând politici, acțiuni, planuri, echipamente, facilități, proceduri, tehnici etc. menite să elimine ori să reducă riscurile privind securitatea și integritatea rețelelor sau a serviciilor de comunicații electronice). Astfel, art. 3 al deciziei menționate prevede:
(1) Furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația de a lua toate măsurile de securitate adecvate pentru a administra riscurile la adresa securității rețelelor și serviciilor de comunicații electronice, astfel încât să asigure un nivel de securitate corespunzător riscului identificat și să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor și rețelelor interconectate, având în vedere cele mai noi tehnologii și, acolo unde este cazul, de a colabora cu alți furnizori pentru implementarea acestor măsuri.
(2) Furnizorii de rețele publice de comunicații electronice au obligația de a lua toate măsurile de securitate necesare pentru a administra riscurile la adresa integrității rețelelor și serviciilor de comunicații electronice, în scopul garantării integrității rețelelor și al asigurării continuității furnizării serviciilor prin intermediul acestor rețele și, acolo unde este cazul, de a colabora cu alți furnizori pentru implementarea acestor măsuri.
(3) Măsurile minime de securitate pe care trebuie să le stabilească și să le implementeze furnizorii, astfel încât să îndeplinească obligația prevăzută la alin. (1) și, după caz, cea prevăzută la alin. (2) vor viza cel puțin domeniile identificate în anexa nr. 1.
(4) Furnizorii au obligația de a evalua și, dacă este cazul, de a actualiza măsurile prevăzute la alin. (3) ori de câte ori este necesar, însă cel puțin o dată la 12 luni.

Capitolele I, II și respectiv III ale Ghidului detaliază cele trei obligații aferente managementului incidentelor cuprinse în Anexa nr.1 a Deciziei nr.512/2013. Scopul acestui Ghid este de a oferi îndrumări furnizorilor de rețele și servicii de comunicații electronice în vederea implementării unor măsuri care să respecte prevederile legale ale deciziei menționate mai sus, contribuind la îmbunătățirea securității și integrității rețelelor și serviciilor de comunicații electronice, din perspectiva managementului incidentelor.

Ghidul oferă îndrumări și recomandări privind implementarea anumitor măsuri, însă alegerea măsurilor specifice aparține furnizorilor de rețele și servicii de comunicații electronice, care vor ține cont în alegerea lor de factori precum rezultatele evaluării riscurilor în cadrul organizației, ale estimării impactului incidentelor asupra furnizării serviciilor de comunicații electronice, profilul organizației (tipurile de rețele și servicii oferite, numărul utilizatorilor de servicii, numărul conexiunilor de acces etc.).

Managementul incidentelor implică dezvoltarea unei politici de management al incidentelor, a unui set de procese și proceduri consistente, repetabile, măsurabile și utilizarea unor mijloace adecvate de natură administrativă, managerială, tehnică sau juridică în vederea detectării, analizei și răspunsului la incidentele ce au loc în cadrul organizației și care afectează/pot afecta procesele și obiectivele afacerii și implicit furnizarea rețelelor și serviciilor de comunicații electronice.

Aplicarea unor procese și proceduri corespunzătoare pentru protecția rețelelor și serviciilor de comunicații electronice, acoperind resurse hardware, software (echipamente de rețea, sisteme, aplicații etc.) și alte tipuri de resurse ce pot fi implicate în procesul furnizării rețelelor și serviciilor de comunicații electronice este menită să conducă la reducerea frecvenței de apariție a incidentelor în cadrul organizației. Prevenirea incidentelor este de regulă mult mai eficientă și mai puțin costisitoare decât răspunsul, reacția la acestea. Astfel, este de regulă util ca organizația să-și orienteze activitățile de tratare a incidentelor nu numai spre acțiuni reactive, ci și spre eforturi proactive.

Ca și principiu general, activitățile de management al incidentelor trebuie corelate cu cele implicate de managementul riscurilor. Astfel, înainte de implementarea unor măsuri de securitate în

[1] http://www.ancom.org.ro/uploads/forms_files/decizie_2013_5121381320491.pdf

domeniul managementului incidentelor, este necesară identificarea și evaluarea riscurilor cu care se confruntă organizația (*risk assessment*).

Este de asemenea util ca măsurile pentru managementul incidentelor să fie stabilite în acord cu documente de standardizare și bune practici în domeniu. Pentru implementarea unor măsuri în domeniul managementului incidentelor pot fi utilizate (parțial, total sau adaptat) documente și publicații de standardizare europene și/sau internaționale precum:

- standarde *ISO*[2] (*ISO/IEC 27035:2011 Information technology - Security techniques - Information security incident management, ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements*, *ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security management, ISO/IEC 27011:2008 Information technology - Security techniques - Information security management guidelines for telecommunications organizations based on ISO/IEC 27002, ISO 22301:2012 Societal security - Business continuity management systems – Requirements etc.)*;

- standarde *ITU*[3] *(ITU-T X.1056 - Security incident management guidelines for telecommunications organizations*);

- standarde/ghiduri *NIST*[4] *(de exemplu NIST SP 800-61 Incident Handling Guide)*;

- standarde/ghiduri/rapoarte *ETSI*[5];

- ghiduri *ISACA*[6];

- ghiduri/studii *ENISA*[7];

- standarde și recomandări *eTOM*[8], *ITIL*[9].

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

[2] International Organization for Standardization
[3] International Telecommunication Union
[4] National Institute of Standards and Technology din Statele Unite ale Americii
[5] European Telecommunications Standards Institute
[6] Information Systems Audit and Control Association
[7] European Union Agency for Network and Information Security
[8] enhanced Telecom Operations Map
[9] Information Technology Infrastructure Library

I. Procese și proceduri privind managementul incidentelor

Conform prevederilor punctului 1 din secțiunea „V. Managementul incidentelor" din Anexa nr.1 la Decizia nr.512/2013, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului au obligația să stabilească procese și proceduri pentru managementul incidentelor care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice (care să vizeze raportarea internă, evaluarea, răspunsul la incidente și escaladarea acestuia), inclusiv prin definirea rolurilor și responsabilităților.

Direcțiile principale ale managementului incidentelor vor fi trasate în cadrul unei politici asociate ce va asigura cadrul pentru dezvoltarea măsurilor în acest domeniu.

Conform bunelor practici în domeniu, organizațiile trebuie să dețină mijloace, instrumente, capabilități/resurse (tehnice, operaționale etc.) necesare pentru a face față oricăror tipuri de evenimente/incidente și/sau amenințări. Printre acestea se pot număra:

- sisteme de detectare a incidentelor (*IDS*[10], *firewall*, *SIEM*[11], *OSS*[12], *senzori, roboți* etc.);

- mijloace/modalități/mecanisme de comunicare/raportare a incidentelor;

- resurse software, hardware, informații etc. pentru analiza incidentelor și răspunsul la acestea (ex. stații de lucru, servere, echipamente de rețea, sisteme de tip *issue tracking*, documentații ale echipamentelor);

- personal cu atribuții în domeniul managementului incidentelor care să aibă alocate roluri și responsabilități specifice.

Pentru eficientizarea managementului incidentelor se va stabili și implementa o schemă ce va cuprinde procese și proceduri documentate, bine structurate, aferente acestui domeniu. Procesele se vor referi la ansamblul etapelor și activităților implicate, iar pe baza acestora vor fi întocmite proceduri aferente. Este recomandabil ca procesul de management al incidentelor să includă următoarele etape:

- detectarea și raportarea internă,
- analiza și evaluarea (inclusiv triere și decizie),
- răspunsul la incidente și recuperarea în urma incidentelor,
- evaluarea și actualizarea măsurilor privind managementul incidentelor.

Activitatea de detectare și raportare implică monitorizarea sistemelor/rețelei/serviciilor. Incidentele trebuie detectate și raportate în timp util pentru a facilita un răspuns eficient.

Analiza și evaluarea incidentelor implică analiza severității și impactului incidentelor asupra proceselor afacerii, implicit asupra furnizării rețelelor și serviciilor de comunicații electronice. Această etapă permite personalului responsabil cu răspunsul la incidente să stabilească prioritățile de răspuns și să determine impactul/efectele incidentelor.

Răspunsul înseamnă remedierea eficientă, în timp util a incidentelor. Recuperarea în urma incidentelor presupune restabilirea proceselor organizației, sistemelor/rețelei/serviciilor afectate în parametrii normali de funcționare.

Politica și schema de management al incidentelor, precum și capabilitățile tehnice și operaționale asociate trebuie evaluate și actualizate ori de câte ori este necesar, în urma unor incidente majore sau pe baza actelor normative aplicabile, dar cel puțin o dată la 12 luni, conform prevederilor art.3, alin (4) din Decizia nr. 512/2013.

Pot fi deprinse multe lecții în urma incidentelor astfel încât organizația poate îmbunătăți măsurile de securitate pentru prevenirea altor incidente, inclusiv schema de management al incidentelor, cât și pentru o mai bună abordare a proceselor implicate.

[10] Intrusion Detection System
[11] Security Information and Event Management
[12] Operations Support Systems

1. Politica de management al incidentelor

Pentru implementarea coerentă și sistematică a managementului incidentelor, este necesar să se întocmească un document privind politica[13] de management al incidentelor în cadrul organizației. Această politică are rolul de a crea cadrul activităților de management al incidentelor ce va sta la baza implementării măsurilor specifice de securitate, de către echipa de răspuns la incidente (capitolul 2), definite prin schema de management al incidentelor de securitate (capitolul 3). La redactarea documentului se va ține cont de rezultatele unui proces premergător de evaluare a riscurilor de securitate, menționat în cadrul secțiunii I din Anexa nr. 1 la Decizia nr. 512/2013.

Documentul de politică de management al incidentelor poate face parte din documentul de politică de securitate a organizației menționat în cadrul secțiunii I de mai sus.

După aprobarea de către conducere, politica va fi disponibilă întregului personal și după caz altor părți.

Se recomandă ca politica de management al incidentelor în cadrul organizației să cuprindă o descriere sumară a anumitor aspecte precum:

a) importanța procesului de management al incidentelor pentru organizație și angajamentul conducerii organizației în sprijinirea managementului incidentelor;

b) scopul, obiectivele și domeniul de aplicare a politicii (cui se aplică, în ce condiții etc.);

c) definirea unor termeni specifici, încadrabili în contextul managementului incidentelor (de exemplu eveniment, incident, incident minor/major/critic, amenințare, vulnerabilitate, răspuns, escaladare, situație de urgență)[14];

d) modul de detectare, raportare și colectare a informațiilor despre evenimentele ce afectează sau care pot afecta securitatea, inclusiv prin corelarea acestor procese cu tipuri de incidente frecvente/predictibile; descrierea va cuprinde un sumar al tipurilor de evenimente posibile, modalitățile/condițiile de detectare și raportare internă a acestora, precum și îndrumări privind detectarea și raportarea unor evenimente noi/impredictibile; descrierea poate cuprinde și un sumar al tipurilor de vulnerabilități și a modului de raportare și tratare a acestora;

e) modul de analiză și evaluare (incluzând triere, prioritizare) a incidentelor;

f) activitățile ce trebuie întreprinse în vederea inițierii răspunsului la incidentele confirmate;

g) necesitatea înregistrării tuturor activităților desfășurate în vederea unor analize ulterioare și păstrarea sigură a evidenței privind incidentele înregistrate;

h) activități post-incident incluzând evaluarea incidentelor și îmbunătățirea proceselor și procedurilor din cadrul schemei de management al incidentelor;

i) activitățile de identificare, raportare și tratare a vulnerabilităților;

j) documentația schemei de management al incidentelor (proceduri, formulare de raportare a incidentelor etc.);

k) personalul care se ocupă de managementul incidentelor/echipa de răspuns la incidente, care poate cuprinde:

- structura organizatorică a personalului cu atribuții în domeniul managementului incidentelor (a echipei de răspuns), inclusiv prin definirea rolurilor și responsabilităților pentru detectare și raportare internă, evaluare/triere și decizie, răspuns, escaladare,

[13] „Politica" desemnează intențiile și direcțiile de acțiune ale unei organizații exprimate în mod oficial de către conducere (*ISO/IEC 27000*).
[14] Conform deciziei nr. 512/2013, un incident reprezintă *acel eveniment care poate afecta sau amenința, direct ori indirect, securitatea și integritatea rețelelor și serviciilor de comunicații electronice; efectele cauzate de lucrările de întreținere a rețelei, programate și anunțate din timp utilizatorilor, nu sunt considerate incidente*.
Amenințarea reprezintă o posibilă încălcare a securității (*ITU-T E.408*).
O vulnerabilitate este un defect sau o slăbiciune a unei resurse sau grup de resurse care poate fi exploatată de una sau mai multe amenințări. Vulnerabilitatea este acea slăbiciune în proiectarea, implementarea, operarea sau controlul intern al unui proces care ar putea expune sistemul la amenințări.

comunicare a informațiilor despre incidente, menținerea relației cu părți externe organizației etc.;

- caracteristici ale personalului cu atribuții în domeniul managementului incidentelor, din punct de vedere al obiectivelor, ariei de activitate și activităților principale ale acestora;
- nivelele de autoritate ale echipei;
- relația cu personalul organizației și cu alte părți;

l) mecanismele, resursele, capabilitățile ce asigură suportul necesar (tehnic, operațional etc.);

m) programul de conștientizare și instruire în domeniul managementului incidentelor;

n) procesul de diseminare a informațiilor despre incidente unor părți externe;

o) actele normative ce trebuie respectate și alte aspecte legale ce trebuie luate în considerare.

2. Echipa de răspuns la incidente

2.1. Structura echipei

În cadrul organizației trebuie să existe personal care să se ocupe de incidentele petrecute pe întreaga durată a acestora (pe parcursul Ghidului, aceasta va fi denumită echipa de răspuns la incidente). Scopul echipei de răspuns la incidente este de a asigura capabilitățile necesare pentru analiza, răspunsul la incidente și îmbunătățirea măsurilor de securitate în urma incidentelor petrecute și pentru coordonarea, diseminarea informațiilor, precum și alte activități implicate în managementul incidentelor.

Dimensiunea, structura, componența echipei de răspuns la incidente trebuie să fie în concordanță cu profilul organizației (ex. organizații de dimensiune redusă, medie, mare).

Din punct de vedere structural, echipele de răspuns pot fi de tipul:

- echipă unică/centrală de răspuns (ex. pentru organizații de dimensiune medie și cu diversitate redusă a resurselor acesteia);

- mai multe echipe de răspuns, cu roluri distribuite pe anumite segmente ale organizației; aceste echipe vor fi coordonate de o singură entitate (ex. pentru organizații de dimensiuni mari și medii);

- personal responsabil cu răspunsul la incidente, implicat și în alte activități (ex. pentru organizații de dimensiune redusă).

Ținând cont de caracteristicile organizației (serviciile de comunicații electronice furnizate, complexitatea rețelei, frecvența și impactul incidentelor și tipul activităților ce trebuie desfășurate în cazul producerii incidentelor), în stabilirea echipei de răspuns organizația trebuie să decidă asupra:

- tipului de echipă necesară (dedicată sau implicată și în alte activități);

- necesității disponibilității membrilor echipei de răspuns (de exemplu 24/7) astfel încât echipa de răspuns să fie capabilă să efectueze în timp util acțiunile de management al incidentelor (disponibilitatea în timp real pentru răspunsul la incidente scade impactul potențial al acestora);

- costurilor implicate în stabilirea și menținerea unor capabilități pentru răspunsul la incidente;

- expertizei necesare echipei de răspuns la incidente (ex. tratarea incidentelor poate necesita cunoștințe tehnice specializate).

În cazul organizațiilor de dimensiuni mari, se recomandă stabilirea unui compartiment dedicat pentru răspunsul la incidente în cadrul organizației. În cadrul acestora există de regulă un compartiment ce se ocupă de operarea rețelei, dar care are și atribuții în domeniul răspunsului la incidente - Centrul de Operațiuni de Rețea (NOC). Acesta poate desfășura de exemplu activități de

monitorizare a rețelelor și de gestionare a incidentelor de rețea. Personalul din NOC are roluri în dispecerizarea alarmelor din teritoriu, escaladarea problemelor către linia necesară de suport, interacțiunea cu echipele locale de suport tehnic etc.. Mai multe informații despre activitatea unui NOC se regăsesc în partea a doua a Ghidului (II. Sistem de detectare a incidentelor), în capitolul dedicat.

În același timp, în funcție de severitatea incidentului, pot fi necesare mai multe nivele de suport pentru tratarea sa (de exemplu nivelul 1 de suport – departamentul IT al organizației, nivelul 2 de suport – alte departamente tehnice, nivelul 3 de suport – producătorii de echipamente și dezvoltatorii de soluții software). Pentru eficientizarea procesului de management al incidentelor, fiecărui nivel de suport îi vor fi asociate serviciile/activitățile necesare pentru managementul incidentelor.

Echipa de răspuns poate cuprinde angajați ai organizației sau organizația poate externaliza anumite sau toate activitățile de răspuns la incidente.

Conștientizarea și instruirea personalului sunt utile pentru succesul unei abordări structurate și planificate a procesului de management al incidentelor. Echipa de răspuns la incidente trebuie să dețină cunoștințe adecvate tratării eficiente a incidentelor. Grupurile de persoane direct implicate în managementul incidentelor pot necesita nivele diferite de instruire în funcție de tipul, frecvența interacțiunii cu schema de management al incidentelor. Se recomandă ca programul de instruire să cuprindă, pe lângă sesiunile teoretice, și exerciții practice, simulări, testări privind schema de management al incidentelor pentru persoanele cheie implicate în proces.

2.2. Roluri și responsabilități

Echipa de răspuns la incidente va respecta politicile, procedurile operaționale, instrucțiunile de lucru în vigoare, aferente mangementului incidentelor, ce sunt stabilite în cadrul organizației.

Aceasta trebuie să aibă responsabilitatea tratării oricăror tipuri de incidente, indiferent de cauză (exemple ale tipurilor de cauză ale incidentelor pot fi eroare umană, eroare de sistem – hardware sau software, fenomen natural, acțiune rău intenționată, cauză externă/parte terță[15]) și de alte caracteristici. O echipă de răspuns trebuie să fie autorizată să ia decizii imediate cu privire la modul de rezolvare a unui incident, să aibă calificarea necesară și competența de analiză și sinteză pentru diagnosticarea și remedierea incidentelor.

Echipa de răspuns la incidente trebuie să decidă imediat asupra modului de tratare a incidentelor, să acorde sprijin prin facilitarea interacțiunii cu alte compartimente sau părți externe, să utilizeze lecțiile învățate în urma incidentelor pentru prevenirea altor incidente similare.

2.3. Servicii

Serviciile reprezintă acele activități ce vor fi desfășurate de către echipa de răspuns la incidente, conform rolurilor și responsabilităților ce îi revin, în vederea managementului incidentelor. Crearea echipei de răspuns la incidente implică și decizia asupra serviciilor pe care aceasta le va desfășura, prin definirea și descrierea acestor servicii. Serviciile vor urmări obiectivele afacerii, implicit furnizarea rețelelor și serviciilor de comunicații electronice.

Serviciile ce pot fi desfășurate de echipa de răspuns la incidente pot fi de detectare a evenimentelor/incidentelor, amenințărilor sau vulnerabilităților, de analiză, de evaluare și triere a incidentelor, de lansare a unor acțiuni de răspuns sau de escaladare. De asemenea, pregătirea, implementarea, testarea instrumentelor și sistemelor necesare managementului incidentelor sunt servicii ce pot fi asigurate de echipa de răspuns la incidente. În vederea îmbunătățirii nivelului de

[15] O definire a acestor tipuri de cauze ale incidentelor, precum şi exemple pentru fiecare categorie se regăsesc în Ghidul de raportare a incidentelor cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice, care este disponibil pe site-ul ANCOM, la adresa: http://www.ancom.org.ro/uploads/links_files/20141219_GHID_DE_RAPORTARE_A_INCIDENTELOR.pdf

securitate în cadrul organizației, echipa poate oferi celorlalți angajați îndrumări privind incidente, vulnerabilități, amenințări, precum și instruire și conștientizare în domeniu.

Aceste servicii pot fi reactive, proactive sau se pot referi la managementul calității securității. Serviciile reactive reprezintă activitățile principale ale echipei și sunt declanșate de vulnerabilități, evenimente sau incidente detectate. Serviciile proactive asigură pregătirea pentru evenimente și incidente, având ca scop reducerea numărului de evenimente și incidente înregistrate. Serviciile privind managementul calității securității măresc aria serviciilor reactive și proactive și pot fi asigurate (și) de alte compartimente ale organizației.

O listă a serviciilor echipei de răspuns la incidente se găsește în Anexa nr.1 la prezentul Ghid. Lista redată nu este exhaustivă, aceasta sintetizează activitățile principale, potențiale ale unei echipe de răspuns la incidente.

2.4. Colaborare

Echipa de răspuns la incidente trebuie să colaboreze cu întreg personalul organizației pentru a detecta, investiga și rezolva incidentele. În acest sens, datele de contact ale membrilor echipei trebuie să fie disponibile întregii organizații.

Pentru analiza incidentelor și găsirea unei soluții de remediere, membrii echipei de răspuns vor solicita, acolo unde este necesar, informații de la diverse compartimente ale organizației.

De asemenea, pentru o derulare operativă a etapei de răspuns la incidente este necesară identificarea din timp a grupurilor din organizație cu care se va coopera pe parcursul derulării acesteia (ex. management, departamente precum IT, juridic, relații publice, departamente tehnice specializate – de exemplu departamente ce se ocupă cu operarea și mentenanța rețelei).

Între părțile implicate în managementul incidentului (inclusiv managementul organizației) trebuie să existe un proces de comunicare eficientă, astfel încât membrii implicați să fie informați cu privire la statusul incidentelor, despre acțiunile desfășurate în diverse etape ale întregului proces de management al incidentelor. Astfel, trebuie să existe reguli de comunicare pe toată durata unui incident care să cuprindă și stabilirea unor mijloace de comunicare (ex. e-mail, telefonic, SMS, conferințe telefonice, întruniri de urgență). Mesajele transmise între părți trebuie să fie clare, complete. Acolo unde este cazul, persoanele care preiau incidentele spre rezolvare de la alte persoane (ex. în cazul schimburilor de tură) vor primi toate informațiile necesare din partea persoanelor inițiale. Nu în ultimul rând, trebuie menținută o colaborare eficientă între personalul echipei de răspuns la incidente aflat în locații diferite (ex. între persoanele aflate la sediul organizației și cele din teren).

De asemenea, trebuie stabilite relații între echipa de răspuns la incidente și părți externe organizației (inclusiv autorități publice responsabile) care ar putea contribui la soluționarea incidentelor și/sau la minimizarea efectelor acestora. Astfel, trebuie stabilite reguli privind relația echipei de răspuns la incidente cu părțile externe relevante care să se refere și la comunicarea informațiilor despre incidente. Măsurile privind comunicarea informațiilor despre incidente unor părți externe sunt tratate în partea a treia a acestui Ghid (III. Proceduri și planuri de comunicare).

3. Schema de management al incidentelor

Conducerea organizației trebuie să stabilească obiectivele managementului incidentelor.

Pentru o tratare cât mai eficientă a incidentelor, organizația trebuie să dețină o schemă de management al incidentelor. Organizația se va asigura că schema de management al incidentelor este în concordanță cu politica de management al incidentelor și cuprinde detalierea proceselor și procedurilor implicate în managementul incidentelor. Astfel, schema de management al incidentelor stabilită în cadrul organizației trebuie să cuprindă procese și proceduri documentate, detaliate, menite să asigure detectarea, analiza, clasificarea, prioritizarea și răspunsul la evenimente, incidente

și vulnerabilități ce afectează sau pot afecta procesele și obiectivele afacerii, implicit securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

Schema va cuprinde inclusiv definirea rolurilor persoanelor responsabile cu managementul incidentelor și asignarea acestor roluri unor persoane/grupuri de persoane adecvate din interiorul organizației și/sau din exterior (membrii echipei de răspuns la incidente și colaboratori). Conducerea organizației trebuie să se asigure că cei răspunzători de managementul incidentelor înțeleg prioritățile organizației referitoare la tratarea incidentelor.

Responsabili pentru activitățile cuprinse în schemă pot fi utilizatori și/sau administratori ai sistemelor, membri ai echipei de răspuns la incidente, conducerea organizației etc.. Aceste persoane pot fi implicate și în activitățile post-incident, precum luarea unor măsuri pentru creșterea nivelului de securitate și prevenirea incidentelor similare, respectiv îmbunătățirea schemei de management al incidentelor. Pot exista situații în care anumite etape ale schemei (de exemplu detectarea evenimentelor de securitate) să intre în responsabilitatea unor părți externe organizației (contractori asociați, furnizori de utilități etc.).

Schema de management al incidentelor poate conține informații sensibile. Stabilirea proceselor și procedurilor din cadrul schemei se va realiza ținându-se cont de confidențialitatea informațiilor.

3.1 Procese corespunzătoare schemei de management al incidentelor

Organizația trebuie să dezvolte procese privind managementul incidentelor, care să descrie activitățile ce trebuie desfășurate pentru rezolvarea incidentelor apărute și pentru prevenirea apariției/reapariției acestora. Un proces poate conține unul sau mai multe subprocese.

Fluxul tratării incidentelor poate diferi de la un incident la altul în funcție de tipurile de rețele, servicii, echipamente, sisteme, aplicații, tehnologii implicate/impactate. În funcție de tipul incidentelor (cauze ce au declanșat incidentul, resurse afectate, părți implicate în procesul de răspuns etc.), două sau mai multe incidente pot implica procese diferite sau activități diferite pentru același proces.

Organizația trebuie să se asigure că funcționarea sistemelor utilizate pentru managementul incidentelor este independentă de funcționarea altor sisteme/echipamente implicate în furnizarea rețelelor și serviciilor de comunicații electronice.

Mijloacele/sistemele tehnice utilizate în procesul de management al incidentelor trebuie testate periodic (inclusiv testarea periodică a echipamentelor de rezervă - back-up).

Printre procesele corespunzătoare schemei de management al incidentelor sunt identificate cele detaliate în continuare (detectare și raportare, evaluare/triere și decizie, răspuns, escaladare, colectarea informațiilor despre incidente și păstrarea evidenței acestora).

3.1.1 Detectare și raportare

Acest proces poate cuprinde subprocese precum:

a) monitorizarea proactivă a indicatorilor specifici

Informațiile despre amenințări, riscuri, vulnerabilități pot fi colectate proactiv, prin monitorizarea și analiza unor indicatori ce pot semnala posibilitatea producerii unor incidente sau posibilitatea exploatării unor vulnerabilități. Astfel de informații prin intermediul cărora se pot preveni sau detecta anumite evenimente sau comportamente neobișnuite ale rețelei sau sistemelor informatice pot proveni, de exemplu, din monitorizarea alarmelor din rețea, a traficului și a log-urilor.

Evenimentele pot fi detectate prin mijloace automate precum sisteme de monitorizare a rețelei, firewall-uri, IDS-uri, sisteme de detectare a codului malițios, sisteme de management al securității, motoare/sisteme de corelare a evenimentelor, urmărirea dezvoltării tehnologiei[16] etc..

Monitorizarea proactivă a indicatorilor specifici presupune totodată și analiza indicatorilor monitorizați.

Prevenirea sau detectarea evenimentelor se poate realiza prin observarea unor aspecte/indicatori specifici de ordin:

- tehnic (de exemplu pe baza schimbării stării normale de funcționare a unui sistem/element de rețea prin observarea unor reacții codificate ale diferitelor sisteme de management al rețelei - mesaje către sisteme de monitorizare, semnalizări acustice și optice etc.);

- fizic (de exemplu observarea unor deficiențe de securitate fizică);

- procedural (de exemplu prin analiza unor date statistice generate de sisteme dedicate/instrumente statistice, pe baza unor indicatori de performanță prestabiliți) etc..

Disfuncționalitățile sau alte comportamente anormale ale sistemelor/rețelelor/serviciilor trebuie atent analizate, întrucât acestea pot constitui indicii ale unor atacuri la adresa securității sau o încălcare reală a securității și trebuie, prin urmare, raportate ca evenimente de securitate.

Degradarea calității este un factor important în detectarea incidentelor de securitate. Mesajele de avertizare/alertele privind scăderea performanței unor servicii, sisteme sau echipamente sunt indicatori ai unor posibile incidente. Aceste mesaje pot proveni de exemplu din reprezentări grafice ale traficului, scripturi, depășiri ale unor praguri prestabilite cu privire la activitatea unor sisteme.

b) identificarea/detectarea apariției evenimentelor/vulnerabilităților (automat sau prin intermediul personalului);

Detectarea se referă la activitățile asociate identificării evenimentelor/vulnerabilităților și monitorizării rețelei, însă nu se limitează la acestea. Persoana din organizație ce a detectat evenimentul de securitate (indiferent de mijloacele de detectare) va iniția procesul de detectare și raportare.

Informațiile despre evenimente pot fi colectate reactiv, prin primirea unor rapoarte/notificări din partea unor surse interne sau externe (automat și/sau prin intermediul personalului). Evenimentele de securitate pot fi detectate din interiorul organizației (de către personal), însă pot exista cazuri în care acestea pot fi detectate din exterior (prin intermediul utilizatorilor de rețele și servicii de comunicații electronice, altor furnizori de rețele și servicii de comunicații electronice interconectați etc.).

Identificarea evenimentelor și vulnerabilităților se poate face cu ajutorul sistemelor de monitorizare a echipamentelor, aplicațiilor, prin accesul direct pe echipamentele de rețea, prin urmărirea rețelei prin intermediul unor sisteme software dedicate, prin primirea în mod automat a unor informații provenite de la senzori, roboți etc..

Personalul organizației trebuie instruit cu privire la acțiunile ce trebuie întreprinse atunci când observă un eveniment. Persoanele care nu fac parte din echipa de răspuns la incidente nu trebuie să încerce acțiuni pe cont propriu pentru confirmarea sau rezolvarea evenimentelor observate.

c) raportarea apariției evenimentelor/vulnerabilităților;

Organizația trebuie să apeleze la un proces de raportare internă a evenimentelor/vulnerabilităților.

Raportarea acestora trebuie să fie responsabilitatea fiecărui utilizator al resurselor organizației și trebuie realizată indiferent de circumstanțe.

Mecanismul de raportare trebuie să fie cât mai ușor, accesibil și disponibil angajaților. Informațiile pot fi transmise sub formă de raport, alertă, notificare etc.. Raportarea se va face, după

[16] Technology Watch

caz, prin mijloace bine definite (de exemplu prin e-mail, SMS sau folosind o aplicație internă). Evenimentele/vulnerabilitățile se pot raporta de exemplu prin completarea unui formular de raportare internă a acestora sau prin intermediul unei platforme dedicate de *ticketing* (prin intermediul căreia se poate vizualiza statusul lor în diferite etape).

Atât acuratețea informațiilor, cât și promptitudinea completării acestora sunt importante. Informațiile cuprinse în raportare trebuie să permită pe cât posibil localizarea evenimentului (din punct de vedere al serviciilor de comunicații afectate, al resurselor afectate și al locației acestora în cadrul rețelei etc.) și să conțină cel puțin data și ora observării/producerii evenimentului, o scurtă descriere a acestuia, persoana care l-a observat, echipamentele afectate. Dacă la momentul detectării evenimentului/vulnerabilității nu sunt disponibile toate informațiile ce îl/o definesc, formularul va fi transmis cu datele avute la dispoziție, urmând ca acestea să fie completate și comunicate persoanelor corespunzătoare imediat ce sunt disponibile.

Se recomandă raportarea evenimentelor suspecte chiar dacă ulterior acestea nu se confirmă ca fiind incidente reale.

Totodată trebuie stabilite părțile care primesc notificările despre evenimente (membrii echipei de răspuns la incidente, conducerea adecvată etc.). Evenimentele pot fi notificate unor persoane/grupuri de persoane diferite, în funcție de tipul acestora. Astfel, pentru fiecare tip de eveniment, se poate desemna o persoană sau un grup de persoane de contact, responsabil cu primirea informațiilor despre evenimentele respective.

În vederea unui management eficient al evenimentelor/vulnerabilităților, trebuie ca angajații să cunoască procesul de raportare. Se recomandă realizarea unor îndrumări/ghiduri privind raportarea diverselor tipuri de evenimente/vulnerabilități. Întreg personalul trebuie să cunoască formatul și modalitatea de raportare a evenimentelor/vulnerabilităților. Atunci când însăși mecanismele destinate comunicării informațiilor despre eveniment/vulnerabilitate sunt sau pot fi afectate, se vor utiliza mijloace alternative (de exemplu dacă serverul de e-mail este afectat de eveniment, se vor utiliza alte mijloace de raportare).

d) primirea rapoartelor privind evenimente/vulnerabilități;

Primirea rapoartelor despre evenimente/vulnerabilități va fi confirmată de către persoanele responsabile din cadrul echipei de răspuns la incidente. Pot fi necesare procese de feedback adecvate pentru ca cei care raportează evenimente/vulnerabilități să fie informați în privința statusului acestora sau a rezultatelor după ce problema a fost rezolvată și închisă. De asemenea, pe durata evenimentului, pot fi necesare mai multe interacțiuni între echipa care se ocupă de tratarea evenimentului/vulnerabilității și persoana care l-a notificat/observat. După caz, echipa de răspuns la incidente va solicita informații suplimentare de la persoanele care le-au notificat.

e) direcționarea evenimentelor/vulnerabilităților către etapa/procesul de evaluare/triere și decizie;

Notificările conținând informații despre evenimente/vulnerabilități detectate vor fi transmise etapei următoare a managementului incidentelor în vederea evaluării/trierii și deciziei asupra acțiunilor de remediere ce trebuie întreprinse.

f) realocarea unor evenimente unor domenii externe procesului de management al incidentelor dacă este cazul și închiderea evenimentelor nedirecționate către etapa următoare.

Unele evenimente pot fi rezolvate local, imediat de către personalul echipei de răspuns. Totodată, unele alerte/alarme se pot dovedi a fi false. În acest sens, trebuie să existe reguli pentru identificarea acestor alarme false și pentru închiderea corespunzătoare a evenimentelor deja soluționate. Acele evenimente care exced aria procesului de management al incidentelor vor fi atribuite domeniilor corespunzătoare.

3.1.2 Evaluare/triere și decizie

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

Acest proces poate cuprinde subprocese precum:

a) analiza și evaluarea inițială a evenimentelor/incidentelor/vulnerabilităților detectate;

Zilnic într-o organizație este posibil să apară foarte mulți indicatori ai unor evenimente. Astfel, este necesar un proces (recomandabil automat) de analiză inițială a acestor semne care să permită selectarea evenimentelor de interes în vederea revizuirii de către personalul adecvat (pentru automatizarea procesului de analiză, poate fi utilă folosirea unui instrument software de corelare a evenimentelor). Organizația se va asigura că toate incidentele vor fi supuse unei evaluări inițiale pentru a determina impactul asupra furnizării rețelelor și serviciilor de comunicații electronice.

După apariția unei alarme sau a unor informări care pot indica prezența unui incident, este necesară o diagnosticare preliminară, corelare a informațiilor disponibile, inclusiv a celor din sistemele de bază implicate, dar și din sistemele auxiliare (ex. climatizare, alimentare cu energie electrică) pentru stabilirea cauzei. Este posibil ca unele incidente (minore) să poată fi rezolvate la această etapă de personalul care primește notificări.

Se recomandă analiza și filtrarea imediată, automată, a alarmelor, pe baza unor grile de evaluare (impact, severitate etc.).

b) strângerea informațiilor despre incidente

Informațiile primite de la persoana/persoanele care au observat/notificat incidentul trebuie completate cu alte informații relevante. Acestea vor fi colectate după caz de la alarme, log-uri, fișiere etc..

c) diagnosticarea incidentelor (stabilirea cauzei);

Diagnosticarea incidentelor se referă la determinarea cauzelor care au dus la producerea acestora. Stabilirea cauzei incidentului ajută la selectarea fluxului de acțiuni care sunt necesare pentru remedierea sa. Pentru diagnosticarea unui incident, trebuie să se analizeze caracteristicile și circumstanțele producerii sale. Fluxul de acțiuni următoare poate fi stabilit mai ușor dacă este vorba de o cauză cunoscută sau observată la alte incidente trecute.

Pentru orice incident petrecut în rețea, personalul specializat trebuie să analizeze cauzele care au dus la apariția sa. De multe ori, aceasta nu este evidentă, cazuri în care se vor analiza informațiile despre incident prin corelare cu alte evenimente pentru a se determina cauza inițială (*root cause*) și efectele subsecvente.

Printre cauzele incidentelor se pot regăsi:

- fenomene naturale/condiții meteorologice nefavorabile (ex. căderi masive de zăpadă, inundații etc.);

- erori de sistem (de exemplu defectarea unor echipamente la nivel hardware sau software);

- erori umane (de exemplu erori în configurarea unor echipamente);

- acțiuni rău intenționate (de exemplu atacuri DoS/SSoS, infiltrarea de malware, vandalism, furturi și distrugeri ale cablurilor de cupru și fibră optică);

- cauze externe/părți terțe (probleme datorate utilităților, de exemplu referitoare la alimentarea cu energie electrică – lipsa tensiunii în rețea/întreruperi și defecțiuni ale surselor de

alimentare cu energie electrică, blocarea unor echipamente din cauza variațiilor tensiunii electrice, lucrări efectuate de terți etc.).

Diagnosticarea poate implica încadrarea incidentelor în anumite categorii (de exemplu incidente de rețea, incidente informatice, incidente datorate alimentării cu energie electrică etc.).

d) identificarea resurselor real sau potențial afectate, precum și localizarea acestora

Analiza incidentului cuprinde și identificarea resurselor ce sunt sau pot fi afectate, cu localizarea cât mai precisă a acestora (la nivel de sisteme, echipamente, componente ale sistemelor, echipamentelor etc.). Se recomandă întocmirea și actualizarea permanentă a unei liste cu resursele/echipamentele ce pot fi afectate de fiecare tip de incidente. O exemplificare în acest sens este redată în continuare[17]:

1. Stații de bază și controlere mobile (BTS, BSC, NodeB, eNodeB, RNC, MME, ANDSF, PCRF);

2. Centre de comutație în rețele mobile (MSC, SGSN, GGSN, PGW, SGW, ePDG sau similar);

3. Regiștrii de localizare în rețele mobile (HLR, VLR, HSS, AuC sau similar);

4. Centre de mesagerie mobilă (SMSC, MMSC);

5. Routere și switch-uri IP (DSLAM, BRAS, Metro router, Metro switch, router, switch, EDGE router, IP PBX, Core router sau similar);

6. Echipamente din noduri de transmisiune (echipamente de modulație/demodulație, echipamente de multiplexare/demultiplexare pe tehnologie SDH, PDH, DWDM, sau similar);

7. Centre de comutație în rețele fixe (Centrală locală/de tranzit/națională/internațională, soft switch, server de gestiune a abonaților);

8. Puncte de interconectare (IXP, POI etc.);

9. Servere de adresare (DHCP, DNS);

10. Sisteme de securitate (IDS, IPS, AAA, LDAP, VPN, firewall etc.);

11. Platforma de taxare;

12. Componente/Platforme de servicii (IPTV, VoIP, IMS, STP, SCP etc.);

13. OSS (Operations Support Systems) și BSS (Business Support Systems);

14. Sisteme de retenție a datelor și interceptare legală a comunicațiilor;

15. Centre de retransmisie de programe media audiovizuale liniare (head-end);

16. Echipamente din rețeaua de distribuție a serviciilor de retransmisie de programe media audiovizuale liniare (amplificatoare, distribuitoare, etc.);

17. Medii de transmisiune: cabluri (cablu torsadat, cablu coaxial, cablu fibră optică etc.), radio (link-uri radio, microunde etc.);

18. Echipamente auxiliare (de alimentare/de backup cu energie electrică, sisteme de răcire etc.).

e) determinarea/evaluarea impactului incidentelor folosind o clasificare/scală[18] agreată (bazată pe definirea unor trepte de severitate) și clasificarea/încadrarea acestora în anumite categorii (de exemplu incidente – minore, majore, critice);

Pentru încadrarea evenimentelor în anumite categorii, trebuie să se determine impactul lor asupra rețelei de comunicații, asupra utilizatorilor de servicii, asupra proceselor afacerii. Pentru estimarea impactului unui incident se pot utiliza grile de încadrare. Determinarea impactului trebuie să țină cont de amploarea evenimentului petrecut (de exemplu din punct de vedere al numărului de conexiuni/utilizatori real sau potențial afectați, al duratei incidentelor, al zonelor geografice afectate, al afectării apelurilor de urgență sau al resurselor hardware sau software afectate - echipamente de rețea, sisteme informatice etc.).

[17] Această listă de resurse și echipamente este utilizată de furnizorii de reţele şi servicii de comunicaţii electronice în raportarea incidentelor cu impact semnificativ către ANCOM, conform Ghidului de raportare a incidentelor cu impact semnificativ asupra furnizării reţelelor şi serviciilor de comunicaţii electronice, disponibil pe pagina web a Autorităţii, la adresa:
http://www.ancom.org.ro/uploads/links_files/20141219_GHID_DE_RAPORTARE_A_INCIDENTELOR.pdf

[18] criteriu de evaluare a impactului stabilit în cadrul managementului riscurilor

De exemplu, evaluarea impactului unui incident care a afectat servicii mobile de comunicații electronice poate cuprinde activități precum identificarea site-urilor afectate de incident, a ariei geografice acoperite de aceste site-uri, distribuția în timp a traficului estimat pentru o perioadă de timp stabilită, identificarea organizațiilor/instituțiilor ce desfășoară activități de interes național ce sunt acoperite de site-urile afectate (de exemplu spitale).

Pentru estimarea numărului de conexiuni afectate de un incident, pot exista metode diferite. O metodă de estimare poate lua în calcul tipul serviciilor de comunicații electronice afectate, fixe sau mobile.

Astfel, pentru estimarea numărului de conexiuni mobile afectate de un incident, se poate utiliza metoda stabilită de ANCOM în Decizia nr.512/2013 (compararea traficului afectat la momentul incidentului cu traficul înregistrat în același interval de timp, în perioada anterioară). Numărul site-urilor afectate este un bun indicator pentru determinarea impactului incidentelor ce afectează serviciile mobile de comunicații electronice.
Pentru estimarea numărului de conexiuni fixe afectate de un incident, metodele de estimare pot implica:

- utilizarea unor instrumente de monitorizare prin care se identifică clienții impactați și corelarea cu răspândirea geografică a clienților care apelează serviciile de call center;

- existența unei corelații între sistemul de facturare și cel de monitorizare, astfel încât la fiecare moment să se cunoască numărul de clienți deserviți de fiecare element de rețea;

- identificarea zonei geografice afectate de un incident prin intermediul sistemului de monitorizare a rețelei și ulterior identificarea numărului de clienți afectați;

- calculul unor medii de clienți afectați în funcție de categoria de rețea, aria geografică și tehnologia afectate.

Pe baza evaluării impactului, se poate realiza o clasificare a incidentelor. Clasificarea incidentelor este utilă pentru stabilirea acțiunilor de remediere necesare. Abordarea în ceea ce privește stabilirea nivelului de severitate a incidentelor/clasificării incidentelor poate fi simplificată (de exemplu cu două nivele) sau amplă. O clasificare/scală amplă poate fi de tipul: incident fără impact, cu impact redus, cu impact mediu, cu impact sever. Impactul incidentului se poate modifica pe parcursul ciclului său de viață.

Exemple de incidente severe pot fi: întreruperea serviciilor de comunicații electronice pentru un număr foarte mare de utilizatori (se are în vedere un prag definit), defectarea completă a unui element important de rețea sau a unui sistem critic (de exemplu routere principale, noduri critice de transmisiuni, sistemul de facturare).

f) corelarea cu alte evenimente/incidente/vulnerabilități trecute sau în curs de desfășurare;

Pentru orice incident trebuie verificată dependența de alte evenimente, incidente sau vulnerabilități. Corelarea acestora poate fi utilă de exemplu în cazul evenimentelor provenite de la mai multe surse, pentru a prioritiza eforturile echipei de răspuns, 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 sporește gravitatea incidentului.

Corelarea evenimentelor/incidentelor trecute sau în curs de desfășurare se poate face ad-hoc sau prin sisteme automate. Se recomandă corelarea prin sisteme automate. Corelarea prin sisteme automate poate implica:

- utilizarea unor platforme de management, aplicații de trouble ticketing;

- observarea simultană a alarmelor provenite de la diverse sisteme de monitorizare;

- utilizarea sistemelor de monitorizare corelate cu sistemul de call center;

- utilizarea unor instrumente dedicate analizei log-urilor de pe echipamente;

- primirea unor informații în mod automat de la sistemele de management centralizat și de la dispeceratele regionale.

Trebuie să se verifice dacă este deschis un alt incident cu aceeași cauză, care a afectat aceleași resurse (elemente de rețea etc.). Dacă există un astfel de incident, se recomandă completarea incidentului deja deschis cu informații suplimentare (dacă este cazul), fără inițierea unui nou incident.

g) prioritizarea incidentelor în vederea răspunsului;

Atunci când se înregistrează mai multe incidente simultan, trebuie stabilite reguli de prioritizare a acestora în vederea implementării răspunsului. Astfel, pentru prioritizarea incidentelor petrecute simultan, este necesară definirea unor nivele de prioritate. Definirea nivelelor de prioritate se poate baza pe impactul incidentului asupra proceselor afacerii, implicit asupra procesului de furnizare a rețelelor și serviciilor de comunicații electronice (dat de regulă de numărul utilizatorilor afectați), pe efortul necesar în vederea răspunsului la incident și recuperării în urma incidentului (de exemplu din punct de vedere al timpului și resurselor necesare recuperării) și pe urgența sa (ce depinde de întârzierea maximă ce poate fi suportată până la rezolvare). Prioritatea incidentelor se poate modifica pe parcursul ciclului de viață al acestora (de exemplu se poate găsi o rezolvare care să permită restabilirea serviciului la un nivel acceptabil, permițând întârzierea închiderii unui incident fără repercusiuni).

h) aflarea unor informații noi despre incidente și evaluări ulterioare;

Poate fi necesară obținerea mai multor informații despre incident în vederea alegerii modului optim de răspuns. În funcție de criticitatea incidentului, pot fi necesare una, două sau mai multe evaluări în vederea clasificării, prioritizării și luării deciziei asupra măsurilor viitoare. Evaluările multiple pot fi realizate de aceleași persoane sau de alte persoane în urma escaladării.

i) analiza posibilităților de răspuns și decizii asupra modului de răspuns la incidente, precum și asupra nivelelor de escaladare;

După încadrarea incidentului într-o categorie, urmează luarea unor decizii în privința pașilor de urmat pentru tratarea sa, de către cine, în ce condiții și cu ce prioritate. Aceste decizii vor implica un proces de asignare a incidentelor către personalul adecvat, de determinare a urgenței tratării și a tipului de răspuns.

Pe baza informațiilor disponibile, se vor identifica și analiza opțiunile de răspuns.

În funcție de dimensiunea organizației și de amploarea incidentelor, pot exista unul sau mai multe niveluri de suport pentru managementul incidentelor, reprezentate de echipa de răspuns la incidente și de colaboratori. În organizațiile de mari dimensiuni pot exista de exemplu două nivele de suport - primul nivel care realizează prima evaluare, ia decizia inițială asupra încadrării incidentului într-o categorie și asupra acțiunilor viitoare și al doilea nivel de suport, responsabil cu a doua evaluare, confirmarea clasificării incidentului și decizia privind modul de răspuns. Ambele nivele de suport pot acționa în sensul remedierii incidentului. Astfel, primul nivel de suport va prelua incidentul în vederea evaluării/trierii. Dacă personalul respectiv are competența necesară, acesta poate remedia incidentul. Incidentele neremediate vor fi transmise celui de-al doilea nivel de suport pentru a doua evaluare și răspuns. Pe baza informațiilor colectate și a rezultatului primelor evaluări și decizii, al doilea nivel de suport va acționa în sensul remedierii incidentului. Nivelele de suport trebuie să fie alese în funcție de natura și complexitatea incidentului. Primul nivel va avea capacitatea tratării incidentelor minore, (de exemplu departamentul IT al organizației), iar ultimul nivel va corespunde incidentelor majore, cu impact sever, care n-au putut fi remediate de celelalte nivele (de exemplu furnizorii de echipamente).

Pentru remedierea anumitor incidente, poate fi necesară implicarea unor părți externe în procesele de management al incidentelor (de exemplu includerea furnizorilor de echipamente în cadrul echipei de răspuns la incidente).

După analiza posibilităților de răspuns, poate fi utilă estimarea perioadei de timp necesară restabilirii serviciilor de comunicații electronice afectate în parametrii normali de funcționare. Aceasta se poate realiza în funcție de factori precum:

- tipul și gravitatea incidentului;

- resursele afectate;

- informațiile despre incident primite de la echipele din teren precum și de la terți;

- capacitatea echipei de răspuns de a remedia incidentul;

- necesitatea deplasării în teren, distanța până la locație și accesul fizic pentru soluționare;

- condițiile meteorologice existente;

- măsurile ce trebuie luate pentru remedierea incidentului și nivelul lor de complexitate etc..

În scopul eficientizării procesului de răspuns la incident este utilă elaborarea unui plan de acțiune. Se recomandă ca astfel de planuri de acțiune să cuprindă cel puțin:

- măsurile de răspuns imediat și cele de răspuns ulterior;

- necesarul de resurse (resurse umane, echipamente etc.).

j) prioritizarea acțiunilor de răspuns;

Pentru facilitarea răspunsului la incident, trebuie utilizat un proces de prioritizare a activităților ce trebuie întreprinse în vederea răspunsului. Pentru prioritizarea activităților de răspuns, trebuie să se aibă în vedere eficientizarea procesului de răspuns astfel încât intervalul de timp necesar remedierii să fie cât mai mic.

k) direcționarea incidentelor către etapa/procesul de răspuns, realocarea unor evenimente unor domenii externe procesului de management al incidentelor și închiderea evenimentelor nedirecționate către etapa următoare, dacă este cazul;

Incidentele vor fi direcționate etapei următoare în vederea acțiunilor de răspuns/remediere deja stabilite. La acest nivel pot exista evenimente care trebuie închise sau realocate unor domenii externe managementului incidentelor.

l) evaluarea vulnerabilităților și luarea deciziilor privind tratarea lor.

Totodată trebuie acordată atenție vulnerabilităților descoperite. În acest sens, pe baza evaluării lor, trebuie luate decizii privind persoanele responsabile pentru tratare, modul optim de tratare, ordinea tratării etc..

3.1.3 Răspuns

Acest proces poate cuprinde subprocese precum:

a) alocarea rolurilor și responsabilităților asociate răspunsului la incidente;

Responsabilitățile în ceea ce privește acțiunile ce trebuie întreprinse pentru răspunsul la incident vor fi repartizate personalului/nivelului ierarhic corespunzător. Pentru eficientizarea procesului de răspuns, poate fi definită o hartă a funcțiilor, compartimentelor interne și părților externe (dacă este cazul) ce vor fi implicate în procesul de răspuns la incidente.

b) asigurarea răspunsului tehnic și managerial;

Acest proces implică acțiuni de rezolvare sau diminuare a efectelor incidentelor, precum și acțiuni de recuperare și restabilire a proceselor sau sistemelor afectate din punct de vedere tehnic (asigurarea instrumentelor și a suportului tehnic necesare remedierii incidentului) și managerial (coordonarea activităților de răspuns).

c) realizarea acțiunilor ce implică răspunsul imediat;

Echipa de răspuns trebuie să identifice și să întreprindă acțiunile de răspuns imediat la incident, să înregistreze toate informațiile aferente și să notifice acțiunile efectuate persoanelor adecvate.

În funcție de gradul de severitate a incidentului, acțiunile de răspuns imediat pot consta în măsuri temporare sau permanente.

Aplicarea unor măsuri temporare reprezintă o modalitate de restabilire parțială a rețelei, serviciilor sau sistemelor afectate. De regulă, dacă particularitățile incidentului sunt cunoscute, fiind facilă identificarea acțiunilor de răspuns necesare, răspunsul imediat este reprezentat de măsuri permanente menite să asigure recuperarea integrală a acestora.

Măsurile imediate sunt de cele mai multe ori necesare pentru evitarea extinderii incidentului sau diminuarea efectelor acestuia. Astfel de măsuri aplicate unor echipamente sau sisteme nu trebuie să afecteze funcționarea celorlaltora cu care sunt corelate. De exemplu, deconectarea de la rețea a unui echipament afectat (ca măsură aferentă răspunsului imediat la incident) nu va afecta funcționarea rețelei în condiții optime. Alte activități de răspuns imediat se pot referi la activarea unor tehnici sau mecanisme (de exemplu pentru detectarea atacatorului).

Ca și exemple de acțiuni pentru răspunsul imediat la incidente pot fi încadrate:

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

- utilizarea soluțiilor de backup/alternative (de exemplu folosirea unor circuite de rezervă/alternative, rerutarea serviciilor pe canale alternative, rerutarea traficului, alimentarea cu energie electrică cu ajutorul generatoarelor);

- izolarea segmentelor de rețea/sistemelor afectate (de exemplu prin dezactivarea unor servicii specifice, adăugarea unor elemente de securitate (routere, firewall-uri etc.) pentru blocarea accesului la alte segmente ale rețelei);

- deconectarea de la rețea a sistemelor afectate (de exemplu în cazul infiltrării în sisteme a unui malware, o măsură imediată ar putea fi deconectarea de la rețea a segmentelor infectate sau a punctelor de acces la rețea asociate);

- scoaterea din rețea a echipamentelor afectate pentru investigații ulterioare și înlocuirea cu echipamente de backup;

- limitarea drepturilor de acces la echipamentele/sistemele afectate (de exemplu schimbarea parolelor);

- limitarea sistemelor afectate (de exemplu în cazul unui atac *DoS* această limitare înseamnă blocarea porturilor asociate atacului sau izolarea accesului dintre segmentele afectate și cele neafectate);

- remedierea problemelor prin aplicarea unor măsuri precum înlocuirea unor echipamente defecte, repararea remote a sistemului sau echipamenului defectat, refacerea traseului de cablu deteriorat sau alte intervenții în cazul distrugerilor sau furturilor de suport de comunicații, depanarea sistemelor informatice, reconfigurarea/reinițializarea unor echipamente sau sisteme software, reconfigurări de parametri, intervenția manuală, relocarea fizică;

- cooperarea cu alte părți - alți furnizori de rețele și servicii de comunicații electronice, furnizori de utilități, producători de echipamente și/sau dezvoltatori de soluții software etc. (de exemplu cooperarea cu furnizori de energie electrică, contactarea producătorilor de echipamente pentru escaladare).

După inițierea răspunsului imediat, trebuie ca echipa de răspuns la incident să verifice dacă incidentul este sau nu sub control. Dacă incidentul se află sub control, după caz, echipa de răspuns va institui activități pentru răspunsul ulterior în vederea închiderii incidentului și restabilirii sistemelor/rețelelor/serviciilor la parametrii normali de funcționare. Dacă incidentul nu este sub control, după caz, echipa de răspuns trebuie să instituie activități de urgență/criză sau de escaladare. Pentru a stabili dacă un incident se află sub control, se poate măsura timpul scurs de la apariția incidentului până la restabilirea în parametrii normali de funcționare. Pe baza rezultatelor managementului riscurilor, se recomandă ca resursele/sistemele/serviciile să aibă o fereastră de timp acceptabilă pentru recuperare. În cazul în care acțiunile de răspuns depășesc acest termen, se consideră că incidentul respectiv nu se află sub control.

Progresul acțiunilor de răspuns trebuie atent monitorizat. Orice dificultate întâmpinată de un membru al echipei de răspuns poate impacta întreg fluxul de lucru, ducând la întârzierea remedierii incidentului.

d) realizarea acțiunilor ce implică răspunsul ulterior;

Dacă incidentul se află sub control, echipa de răspuns trebuie să identifice acțiunile ulterioare de răspuns în vederea restabilirii sistemelor/rețelelor/serviciilor la parametrii normali de funcționare, iar persoanele responsabile de aceste acțiuni vor fi notificate în consecință. După ce acțiunile au fost întreprinse, incidentul va fi închis și persoanele din conducere vor fi notificate în acest sens.

O arie de răspunsuri ulterioare se poate referi la luarea unor măsuri pentru prevenirea apariției unor incidente similare. De exemplu, dacă un incident a fost cauzat de o eroare de sistem (hardware sau software), va fi contactat producătorul de echipamente și/sau soluții software pentru identificarea unor soluții de răspuns ulterior. Dacă a fost implicată o vulnerabilitate, trebuie luate măsuri pentru minimizarea acesteia. Acțiunile de răspuns la incident vor ține cont de efectul incidentului asupra tuturor resurselor afectate (de exemplu în cazul unui incident a cărui cauză a fost configurarea eronată a unui software, trebuie avute în vedere verificarea configurațiilor adiacente, schimbarea unor parole etc.).

Altă arie de activitate se poate referi la restabilirea sistemelor/rețelelor/serviciilor în parametrii normali de funcționare prin aplicarea unor măsuri corespunzătoare și/sau monitorizarea sistemelor/rețelelor/serviciilor. După rezolvarea incidentului, pot fi implementate măsuri privind monitorizarea sistemelor pentru detectarea unor comportamente neobișnuite/suspicioase ale sistemelor/rețelelor ce ar putea declanșa alte incidente și pentru identificarea unor sisteme afectate de incident ce nu au fost încă descoperite. Răspunsul ulterior, pe termen lung la incidente, poate implica acțiuni precum:

- acțiuni de remediere/restabilire completă a sistemelor/rețelelor/serviciilor afectate;

- implementarea unor măsuri tehnice și organizatorice pentru prevenirea altor incidente similare și actualizarea măsurilor tehnice existente (de exemplu achiziționarea de echipamente pentru înlocuirea celor afectate, actualizarea proceselor, politicilor și procedurilor operaționale, implementarea unor soluții de back-up, schimbarea tehnologiilor/soluțiilor tehnice, contractarea unor servicii, modificări în configurația rețelei pentru minimizarea impactului unui potențial incident, îmbunătățirea mecanismelor de detectare a incidentelor, implementarea unor măsuri de securitate fizică pentru zone/clădiri/centre de comunicații, dar și încăperi dedicate activităților implicate de furnizarea rețelelor și serviciilor de comunicații electronice, implementarea de noi platforme de servicii sau elemente de rețea, schimbarea vendorului de echipamente sau platforme de servicii);

- analize post-incident și verificarea/monitorizarea sistemelor/rețelelor/serviciilor (de exemplu analiză post-incident care conține cauza incidentului, modul de soluționare și acțiuni post-incident pentru evitarea incidentelor de același tip, testarea preventivă a sistemelor neafectate, simulări de atacuri cibernetice, evaluarea riscurilor, urmărirea modului de funcționare a sistemelor și echipamentelor implicate pe o anumită perioadă de timp, monitorizarea soluțiilor adoptate pentru răspunsul la incidente).

Măsurile ce constituie soluția definitivă de remediere a incidentului sunt obligatorii, acestea având scopul restaurării funcționării rețelei la parametrii tehnici și calitativi anteriori producerii incidentului.

Restabilirea funcționării serviciilor/sistemelor/echipamentelor în parametrii normali de funcționare închide fluxul de tratare a incidentului. Aici este inclusă și verificarea funcționalităților sistemelor.

e) realizarea activităților necesare în caz de urgență/criză (eventual prin escaladarea la personalul corespunzător) sau în cazul unui impact major/sever asupra organizației/furnizării rețelelor și serviciilor de comunicații electronice;

Activitățile de criză se pot referi la activarea unor proceduri/planuri de acțiune în cazul unor incendii, cutremure și alte dezastre naturale sau provocate de oameni. În aceste cazuri poate fi necesară activarea unor răspunsuri specifice, documentate, de exemplu în planurile de continuitate

și de recuperare, prin utilizarea unor instrumente, proceduri sau planuri prestabilite. Astfel, dacă incidentul a dus la perturbări grave ale funcționării rețelei sau serviciului, activitățile de recuperare pot implica activarea planurilor de continuitate și de recuperare. Organizația trebuie să identifice opțiuni de tratare a unor incidente ce cauzează perturbări grave ale funcționării rețelei sau serviciului în cadrul strategiei pentru asigurarea continuității furnizării rețelelor și serviciilor de comunicații electronice, respectiv în planurile de continuitate și recuperare. Aceste opțiuni vor ține cont de prioritățile afacerii/impactul incidentului asupra furnizării rețelelor și serviciilor de comunicații electronice, luând în calcul termenele de recuperare.

Strategia pentru asigurarea continuității furnizării rețelelor și serviciilor de comunicații electronice în situațiile generate de perturbări grave ale funcționării rețelei sau serviciilor, capabilitățile de implementare a strategiei și planurile de continuitate și recuperare fac obiectul obligațiilor privind implementarea măsurilor de securitate în domeniul managementului continuității afacerii, impuse furnizorilor prin Decizia nr.512/2013.

Situațiile generate de perturbări grave ale funcționării rețelelor și serviciilor trebuie tratate cu maximă prioritate. După implementarea soluției agreate, se va verifica eficiența sa. Dacă se dovedește că soluția nu este eficientă, incidentul se va reanaliza și se va agrea o nouă soluție.

În cazul incidentelor critice se recomandă constituirea unor echipe speciale care să funcționeze pe durata incidentului (de exemplu așa numite „celule de criză").

În vederea răspunsului la incidente majore, poate fi utilă stabilirea unei locații în interiorul organizației pentru desfășurarea activităților de recuperare. Echipa de răspuns se va întruni în această locație la intervale de timp planificate pentru a dezbate opțiunile de tratare a incidentului, prioritizarea acțiunilor de răspuns, soluții alternative de răspuns etc..

f) realocarea evenimentelor unor domenii externe procesului de management al incidentelor dacă este cazul și închiderea răspunsului/incidentului;

După rezolvarea incidentului (inclusiv restabilirea serviciului în parametrii inițiali) și înregistrarea tuturor informațiilor asociate, incidentul va fi închis corespunzător. Se va ține cont de aspectele nesoluționate (eventual riscuri reziduale), luându-se în calcul încadrarea acestora în diverse domenii externe procesului de management al incidentelor în vederea remedierii. După realizarea acțiunilor de răspuns necesare, în vederea confirmării remedierii incidentului, trebuie efectuate testări corespunzătoare. Incidentul se închide doar după confirmarea remedierii sale. Închiderea incidentului trebuie urmată de transmiterea unor notificări în acest sens părților implicate, inclusiv persoanei care a raportat incidentul și persoanelor a căror activitate este impactată de acțiunile corective. Dacă remedierea nu este confirmată după parcurgerea tuturor pașilor planificați, incidentul va fi reasignat personalului corespunzător (eventual escaladat) pentru o nouă analiză și diagnosticare.

g) corelarea și monitorizarea continuă a activităților de răspuns, concomitent cu verificarea statusului incidentului în vederea stabilirii dacă acesta este sau nu ținut sub control;

Pentru eficientizarea procesului de răspuns, pe durata incidentului, activitățile de răspuns vor fi corelate corespunzător. Se recomandă supravegherea/monitorizarea acestor activități, inclusiv prin observarea momentelor de timp asociate întreprinderii diferitelor acțiuni, astfel încât să existe un control permanent al stării incidentului.

h) monitorizarea rețelei/sistemelor/serviciilor după restabilirea funcționării acestora la parametri normali;

După punerea în funcțiune a serviciilor/sistemelor/echipamentelor afectate, funcționarea acestora trebuie atent supravegheată o anumită perioadă de timp pentru a se asigura recuperarea completă și tratarea corespunzătoare a riscurilor, amenințărilor și vulnerabilităților evidențiate de producerea incidentului în cauză.

i) tratarea vulnerabilităților;

Etapa de răspuns trebuie să cuprindă și răspunsul la eventualele vulnerabilități care au dus la producerea incidentului. Implementarea măsurilor de tratare a vulnerabilităților trebuie să urmeze proceselor privind managementul schimbărilor. Astfel de măsuri pot fi substanțiale (de exemplu upgrade-uri software).

3.1.4 Escaladare

Pentru o gestionare cât mai eficientă a incidentelor ce necesită escaladare, în cadrul organizației trebuie stabilite reguli de escaladare și trebuie definite praguri de escaladare.

Escaladarea se realizează după caz:

- în vederea luării unei decizii în privința acțiunilor ce trebuie întreprinse pentru tratarea unui incident (escaladare ierarhică[19]);

- atunci când sunt necesare investigații sau acțiuni suplimentare din partea altor persoane/grupuri de persoane specializate (escaladare funcțională[20]).

Escaladarea ierarhică poate fi declanșată atunci când pentru rezolvarea incidentului sunt necesare decizii din partea unui management superior (acesta poate angrena resurse sau competențe suplimentare pentru rezolvarea incidentelor).

Escaladarea ierarhică înseamnă escaladarea în luarea deciziilor privind modul de încadrare a evenimentelor în anumite categorii prestabilite, de prioritizare a activităților de răspuns pentru un anumit incident sau în ceea ce privește tipul acțiunilor de remediere/răspuns. Escaladarea ierarhică poate fi necesară în cazul incidentelor critice, la depășirea unor praguri de timp prestabilite și asociate severității incidentului, în funcție de nivelul afectării *SLA* etc..

Escaladarea funcțională înseamnă transferul unui incident către o echipă tehnică cu un alt nivel de expertiză în cazul în care incidentele depășesc competențele tehnice sau operaționale ale echipei inițiale.

În funcție de tipul incidentului, echipa de răspuns la incidente poate escalada incidentul altor persoane din interiorul organizației în vederea răspunsului. De asemenea, activitățile necesare în situații de urgență/criză pot fi realizate prin escaladarea la personalul corespunzător. Pot exista cazuri în care incidentele nu pot fi remediate în interiorul organizației și necesită a fi externalizate. Un exemplu în acest sens poate fi defectarea unui echipament sau sistem software ce nu poate fi remediată de personalul organizației și trebuie escaladat producătorului/furnizorului de echipament sau sistem software pe baza unor contracte/înțelegeri agreate. În astfel de cazuri, personalul organizației monitorizează activitățile părților externe implicate, precum și progresul acestora. După escaladare, aceștia vor avea sprijinul echipei de răspuns la incidente.

Pot exista mai multe niveluri de escaladare funcțională, de exemplu: nivelul 1 – incidente ce pot fi tratate și remediate de persoana/echipa care le-a detectat, nivelul 2 – incidente ce necesită colaborare din partea unor echipe de experți, nivelul 3 – incidente ce necesită colaborare din partea unor echipe din teren, nivelul 4 – incidente ce necesită colaborare din partea furnizorilor sau producătorilor de echipamente).

Escaladarea poate fi necesară pe toată perioada desfășurării incidentului. De exemplu, escaladarea poate interveni în timpul sau în urma evaluărilor și deciziilor din cadrul fazei de evaluare/triere și decizie (escaladarea ierarhică sau funcțională a deciziilor) sau chiar în timpul răspunsului la incident (escaladarea ierarhică sau funcțională a acțiunilor de răspuns).

În vederea escaladării, după caz, managerul echipei de răspuns va colabora cu managementul corespunzător și cu alte părți interne sau externe. Condițiile și circumstanțele acestor colaborări trebuie, pe cât posibil, prestabilite.

[19] Escaladarea ierarhică este cunoscută şi sub denumirea de escaladare administrativă.
[20] Escaladării funcţionale îi este asociată şi denumirea de escaladare tehnică.

3.1.5 Colectarea informațiilor despre incidente și păstrarea evidenței acestora

Păstrarea evidenței incidentelor se referă la păstrarea unor documente, înregistrări (log-uri) referitoare la incidente și la arhivarea informațiilor despre incidente.

Trebuie acordată atenție păstrării evidenței dovezilor ce au dus la confirmarea incidentelor.

Se recomandă colectarea informațiilor despre toate incidentele petrecute, nu numai despre incidentele majore/critice.

Pentru evidență, se recomandă întocmirea unor rapoarte individuale ale incidentelor care să includă informații privind incidentul pe parcursul tuturor etapelor/proceselor schemei de management.

În vederea întocmirii rapoartelor individuale, se recomandă identificarea unui set de elemente ce vor fi colectate pentru fiecare incident major/stabilirea unor formulare adecvate. Aceste elemente pot include:

- impactul incidentului asupra proceselor afacerii, implicit asupra furnizării rețelelor și serviciilor de comunicații electronice;

- momentele cheie ale incidentului (momentul producerii, detectării, încheierii incidentului etc.);

- cauza/cauzele ce au condus la producerea incidentului;

- locația incidentului (aria geografică afectată, dar și identificarea locației resurselor afectate);

- descrierea resurselor afectate;

- alte incidente/evenimente asociate/corelate;

- rezultatele evaluării incidentului;

- deciziile luate în vederea răspunsului la incident;

- acțiunile întreprinse în vederea remedierii incidentului/fluxul de lucru de la detectare până la remedierea incidentului;

- acțiunile planificate pentru recuperarea integrală în urma incidentului și pentru prevenirea altor incidente similare;

- comentarii ale personalului responsabil cu managementul incidentelor;

- informații de contact ale părților implicate – ale celui ce detectează/raportează incidentul și ale celui/celor ce se ocupă de tratarea acestuia;

- statusul incidentului în diferite etape/momente de timp pe tot parcursul desfășurării sale ce va fi actualizat după fiecare proces/activitate; dacă gradul de severitate a incidentului se modifică pe parcursul tratării sale sau se obțin informații actualizate despre incident, toate informațiile vor fi consemnate;

- cuantificarea costurilor implicate de rezolvarea incidentului;

- lecții învățate etc..

Astfel de rapoarte vor fi actualizate ori de câte ori va fi necesar. Actualizările vor acoperi activitățile întreprinse până la acel moment. În funcție de incident, aceste rapoarte pot fi întocmite în timpul derulării activităților de tratare sau după rezolvarea incidentului în cauză (rapoarte post-incident). Colectarea informațiilor sprijină celelalte procese privind managementul incidentelor. Formularele de raportare a incidentelor pot fi utilizate pentru evidența incidentelor. Acestea vor fi completate și actualizate cu informații privind incidentul în diverse etape ale schemei de management.

În funcție de frecvența incidentelor din rețea, se pot întocmi rapoarte periodice zilnice, săptămânale, lunare etc..

Se recomandă implementarea unor instrumente tehnice și operaționale de colectare a incidentelor și vulnerabilităților care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

Urmărirea automată a evoluției incidentelor și vulnerabilităților poate permite o evidență clară a acțiunilor întreprinse, inclusiv prin indicarea persoanelor implicate în aceste acțiuni.

Se recomandă păstrarea unui centralizator care să conțină toate informațiile despre incidentele petrecute în cadrul organizației. Acesta trebuie să permită compararea și analiza acestora din diferite perspective și să ofere o imagine cât mai clară asupra amenințărilor, vulnerabilităților, riscurilor la adresa rețelelor și serviciilor de comunicații electronice. Acest centralizator trebuie să permită securizarea informațiilor colectate și arhivarea acestora.

De exemplu, centralizatorul incidentelor poate fi integrat aplicației de ticketing a organizației.

Pentru analize ulterioare, în vederea justificării îndeplinirii unor obligații legale sau pentru conformitate și audit, în cadrul organizației trebuie păstrată evidența activităților asociate managementului incidentului, cu monitorizarea acestei evidențe. Evidența activităților derulate în vederea remedierii poate presupune înregistrarea acțiunilor propriu-zise realizate, cu indicarea datei și orei acțiunilor, mijloacelor și instrumentelor utilizate etc.. În cadrul organizației trebuie păstrate înregistrări privind statusul incidentelor în diferite etape ale ciclului lor de viață. Utilizarea unor aplicații și sisteme de tip *issue tracking* poate facilita această evidență și poate contribui la rezolvarea incidentelor în timp util.

Totodată, trebuie păstrate înregistrări privind vulnerabilitățile identificate în cadrul rețelei de comunicații, care să indice modalitatea de soluționare a acestora, dacă au fost diminuate, eliminate etc..

Atunci când în urma incidentului trebuie aplicate măsuri disciplinare, legale sau trebuie solicitate anumite despăgubiri, trebuie avute în vedere măsuri pentru colectarea și securizarea de dovezi în conformitate cu clauzele legale, contractuale sau procedurale aplicabile.

Perioada păstrării evidenței incidentelor este de asemenea importantă. În acest sens, se vor respecta normele interne de păstrare și arhivare.

3.1.6 Automatizarea proceselor corespunzătoare schemei de management al incidentelor

Se recomandă automatizarea proceselor privind managementul incidentelor. De exemplu, pentru procesul de detectare și raportare internă, automatizarea se poate referi la existența unor sisteme de monitorizare a elementelor rețelei de comunicații electronice (monitorizarea alarmelor generate de elementele de rețea).

3.2 Proceduri corespunzătoare schemei de management al incidentelor

În cadrul organizației, trebuie stabilite proceduri documentate (care să cuprindă inclusiv roluri și responsabilități asociate) pentru managementul eficient al incidentelor și vulnerabilităților. Astfel de proceduri vor acoperi toate procesele din cadrul schemei de management al incidentelor, respectiv activitățile personalului implicat în analiza și răspunsul la incidente, inclusiv ale personalului implicat în rezolvarea unor situații de urgență generate de perturbări grave ale funcționării rețelelor.

O procedură documentată privind managementul incidentelor poate acoperi unul sau mai multe procese din cele descrise în capitolul dedicat.

Unele activități privind managementul incidentelor pot fi incluse și în alte proceduri/politici (de exemplu activitățile pentru rezolvarea unor situații de urgență pot fi cuprinse în planul de continuitate a afacerii).

Totodată, procedurile vor respecta politica de management al incidentelor și după caz alte documentații relevante asociate procesului de management al incidentelor.

Procedurile corespunzătoare schemei de management al incidentelor trebuie să se adreseze tuturor participanților în procesul de management al incidentelor (personalului organizației - din toate sediile ce aparțin organizației, contractorilor, persoanelor care desfășoară temporar activități asociate managementului incidentelor în cadrul organizației, celor care au drept de acces la distanță la infrastructura organizației etc.). Nu toate procedurile din cadrul procesului de management al incidentelor necesită a fi cunoscute și înțelese de către întreg personalul organizației (de exemplu cele referitoare la activitățile interne ale echipei de răspuns la incidente). Anumite documente de interes (ce conțin îndrumări în cazul unor incidente etc.) vor fi disponibile personalului.

Procedurile vor acoperi tratarea incidentelor predictibile, potențiale, cunoscute, dar și a celor excepționale, necunoscute.

În funcție de riscurile identificate, procedurile de management al incidentelor pot trata toate tipurile de incidente sau pot exista proceduri distincte pentru tratarea diverselor tipuri de incidente. De exemplu, procedurile pot diferenția incidentele în funcție de:

- tipul incidentelor (incidente de rețea, incidente de securitate fizică (acces neautorizat în incinta organizației etc.), incidente cibernetice etc.);

- nivelul lor de criticitate (incidente minore, incidente majore, incidente critice etc.);

- resursele ce pot fi afectate;

- cauzele incidentelor;

- părțile implicate în tratarea/remedierea acestora.

O procedură privind managementul incidentelor trebuie să cuprindă cel puțin scopul procedurii, definirea unor termeni de referință pentru managementul incidentelor, descrierea activităților ce trebuie întreprinse în sensul îndeplinirii scopului procedurii și părțile implicate în aceste activități, cu asignarea acestora pentru fiecare activitate.

De asemenea, procedurile vor conține referințe la alte documente interne cu care sunt corelate sau trimiteri la documente externe asociate (de exemplu documente de standardizare precum *ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements*, *ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security management*), ce pot contribui la o cât mai bună înțelegere a procedurilor respective. Printre alte documente interne relevante, se pot regăsi politica de securitate a organizației, proceduri sau metodologii interne privind managementul riscului.

În cadrul procedurilor se recomandă diferențierea diferitelor părți implicate în procesul de management al incidentelor (de exemplu angajați ai organizației, echipa de răspuns la incidente, conducere, departamentul IT, alte departamente etc.). Pentru fiecare parte implicată, procedurile vor cuprinde alocarea rolurilor și responsabilităților corespunzătoare, prin specificarea sarcinilor ce îi revin în procesele urmărite.

Pentru o mai bună înțelegere a fluxului de lucru, descrierea activităților poate fi însoțită de diagrame de lucru. Astfel, procedurile pot cuprinde formulare dedicate, diagrame de lucru sau de proces, scheme logice care să prezinte cât mai eficient fluxul de lucru și în special succesiunea activităților ce trebuie întreprinse de personalul implicat în managementul incidentelor.
Procedurile pot cuprinde definirea unor riscuri ce pot interveni pe parcursul desfășurării activităților aferente managementului incidentelor, cu precizarea modalităților în care se pot controla aceste riscuri.

4. Evaluarea schemei de management al incidentelor și îmbunătățiri

În urma analizei incidentelor petrecute în cadrul organizației, pot fi deprinse lecții aplicabile întregului domeniu al managementului incidentelor (politicii aferente, proceselor și procedurilor schemei de management al incidentelor etc.).

De asemenea și alte domenii de securitate pot fi îmbunătățite (de exemplu prin stabilirea unor măsuri în sfera managementului riscurilor sau revizuirea politicii de securitate a organizației) în același context.

Totodată, trebuie implementate mecanisme pentru a determina, măsura și monitoriza tipul, volumul incidentelor, respectiv costurile implicate în acțiunile de răspuns și/sau prevenire a unor incidente similare. Astfel de instrumente pot consta de exemplu în rapoarte periodice privind incidentele, sisteme de *ticketing* electronic ce permit urmărirea tuturor incidentelor de la apariție până la remediere, analize statistice, software dedicat pentru managementul incidentelor.

4.1 Analiza incidentelor și organizarea unor întâlniri

Se recomandă ca organizația să analizeze periodic informațiile din centralizatorul incidentelor și vulnerabilităților pentru a identifica tendințele incidentelor și domeniile ce necesită atenție specială, măsurile ce pot fi luate pentru prevenirea unor incidente similare, cât și pentru a determina și corecta deficiențele proceselor și procedurilor de management al incidentelor.

În vederea analizei incidentelor trebuie organizate întâlniri periodice de diseminare a informațiilor, cel puțin după incidentele majore. Întâlnirile după incidentele majore vor reuni membri ai echipei de răspuns la incidente, precum și alte persoane implicate în procesul de management al incidentelor. Întâlnirea ce urmează incidentului trebuie să aducă în atenție răspunsuri la întrebări precum:

- ce s-a întâmplat cu exactitate (care a fost cauza incidentului, impactul său etc.);

- dacă informațiile despre incident au fost suficiente și cum ar putea fi obținute informații suplimentare în alte cazuri;

- dacă incidentul a fost tratat eficient (dacă pașii urmați au condus la remedierea incidentului în timp util);

- dacă procedurile documentate au fost respectate;

- dacă documentația existentă a acoperit toate cerințele necesare remedierii incidentului și cum poate fi îmbunătățită această documentație (proceduri operaționale, instrucțiuni de lucru etc.);

- dacă toate părțile implicate au fost informate de statusul incidentului;

- dacă au fost luate măsuri pentru prevenirea unor incidente similare;

- cum ar trebui să se acționeze într-o situație viitoare similară;

- ce acțiuni suplimentare referitoare la incident ar putea fi întreprinse (de exemplu alertarea unor părți externe privind existența unei vulnerabilități, transmiterea unor notificări către alte părți pentru prevenirea unor incidente similare);

- ce etape/procese ar putea fi îmbunătățite în cazul altor incidente;

- ce acțiuni corective ar putea preveni producerea unor incidente similare;

- ce indicatori trebuie urmăriți pentru prevenirea altor incidente;

- ce alte instrumente/resurse sunt necesare pentru detectarea, analiza și răspunsul la incidente viitoare;

- dacă există lecții învățate ce ar trebui documentate.

De asemenea, se recomandă organizarea unor întâlniri periodice, în care să se analizeze incidentele pe o anumită perioadă anterioară (de exemplu organizarea unei întâlniri la începutul anului în care va fi analizată situația incidentelor înregistrate de organizație pe al doilea semestru al anului anterior). Pe lângă membrii echipei de răspuns la incidente și alte persoane implicate în procesul de management al incidentelor, este recomandabil ca la întâlnirile periodice să participe și reprezentanți ai managementului organizației. În cadrul acestor întâlniri se dezbat aspecte și concluzii legate de incidentele petrecute, acțiunile întreprinse pentru rezolvare și lecțiile ce pot fi învățate. Informațiile obținute de pe urma evaluării incidentelor pot fi utile pentru identificarea

cauzelor frecvente ale acestora, precum și a incidentelor care se repetă sau au un impact puternic asupra organizației, asupra furnizării rețelelor și serviciilor de comunicații electronice. Trebuie luată în calcul situația în care (în mod repetat) se înregistrează mai multe incidente al căror impact individual nu este unul puternic, însă prin repetarea acestora impactul cumulat se accentuează, atingând amploarea unui incident major.

Se recomandă întocmirea unor rapoarte anuale interne privind incidentele înregistrate în cadrul organizației, care să cuprindă statistici privind incidentele (a se vedea caracteristicile menționate în cadrul capitolului 3.1.5 Colectarea informațiilor despre incidente și păstrarea evidenței acestora din prima parte a Ghidului).
Astfel de rapoarte pot oferi o imagine de ansamblu în ceea ce privește nivelul global al securității rețelelor și serviciilor de comunicații electronice în cadrul organizației, pot sprijini procesul de management al incidentelor și pot reprezenta un punct de plecare în implementarea unor noi măsuri de securitate.

4.2 Evaluarea schemei de management al incidentelor

Pentru evaluarea schemei de management al incidentelor, organizația trebuie să măsoare periodic (cel puțin anual) eficacitatea proceselor și procedurilor de management al incidentelor.

Pot exista mai multe metode de măsurare a eficacității proceselor și procedurilor de management al incidentelor. Printre aceste metode se regăsesc următoarele:

- evaluarea fluxului de tratare a incidentelor cu impact semnificativ;

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

- măsurarea unor indicatori de performanță operațională, organizatorică și a gradului de îndeplinire a indicatorilor și obiectivelor prestabilite;

- audit intern *SMSI*[21] și analiză *SMSI*.

Organizația trebuie să verifice și să testeze periodic procesele și procedurile aferente managementului incidentelor pentru a identifica problemele potențiale ce pot apărea pe parcursul derulării activităților efective. În acest sens se recomandă organizarea unor testări periodice pentru verificarea acestor procese și proceduri și pentru verificarea modalității de răspuns la incidente. Astfel de testări se pot referi la simulări ale unor posibile atacuri, erori sau disfuncționalități ce pot apărea, cu asigurarea faptului că sistemele nu vor fi afectate de aceste simulări. În vederea realizării acestora se vor crea scenarii de incidente pe baza vulnerabilităților, amenințărilor și riscurilor identificate (rezultate în urma evaluării riscurilor) la adresa securității și integrității rețelelor și serviciilor de comunicații electronice. Sistemele și echipamentele critice sau care stochează și prelucrează informații sensibile vor fi testate suplimentar. Testarea poate avea ca rezultat modificarea schemei de management al incidentelor.

4.3 Îmbunătățiri ale măsurilor de securitate

În urma analizei incidentelor prezentată la 4.1 și a evaluării schemei de management al incidentelor prezentată la 4.2, poate rezulta necesitatea unor îmbunătățiri de ordin tehnic sau organizatoric ale măsurilor de securitate.

Pot fi necesare îmbunătățiri ale politicii de management al incidentelor, în ceea ce privește compartimentul de tratare a incidentelor (modificări asupra structurii echipei de răspuns la incidente, asupra rolurilor și responsabilităților atribuite etc.) sau asupra schemei de management al incidentelor (actualizarea proceselor și procedurilor aferente).

[21] Sistem de Management al Securității Informației

Suplimentar față de îmbunătățirile aduse managementului incidentelor, este necesară evaluarea procesului de management al riscurilor cu luarea în considerare a amenințărilor și vulnerabilităților descoperite. Ca urmare a evaluării riscurilor, poate fi necesară modificarea unor măsuri existente sau implementarea altora noi și în alte domenii (politica de securitate și managementul riscului, securitatea resurselor umane, securitatea și integritatea rețelelor, a facilităților asociate și a informațiilor, managementul operațiunilor, managementul continuității afacerii, monitorizare, testare și audit etc.).

Pot exista măsuri care nu pot fi implementate imediat, deoarece, de exemplu, nu sunt fezabile din punct de vedere financiar sau operațional, situație în care acestea vor figura în obiectivele pe termen lung ale organizației (de exemplu înlocuirea unor echipamente de securitate cu altele având caracteristici tehnice superioare).

Pentru o bună evidență, rezultatele evaluării incidentelor și a procesului de management al incidentelor vor fi documentate, iar schimbările asupra proceselor și procedurilor vor fi testate înainte de aplicare.

II. Detectarea incidentelor

Conform prevederilor punctului 2 din secțiunea „V. Managementul incidentelor" din Anexa nr.1 la Decizia nr.512/2013, furnizorii au obligația să stabilească un sistem de detectare a incidentelor.

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

Un sistem de detectare a incidentelor reprezintă ansamblul elementelor interdependente, între care se stabilește o interacțiune dinamică pe baza unor reguli prestabilite, în scopul atingerii obiectivului fundamental – detectarea incidentelor și vulnerabilităților ce afectează sau pot afecta securitatea și integritatea rețelelor și serviciilor de comunicații electronice, mai precis procesul furnizării acestora către utilizatorii finali. Acest sistem poate reuni mai multe tipuri de resurse – umane (cu roluri și atribuții distribuite), tehnice (cu funcționalități și capabilități definite), operaționale etc.. Sistemul de detectare poate fi asimilat diverselor tipuri de metode de detectare a incidentelor și vulnerabilităților, unele dintre acestea fiind descrise pe parcursul acestui capitol. Complexitatea sistemului de detectare (din punct de vedere al resurselor implicate sau al funcționalităților sale) poate diferi în funcție de particularitățile organizației (din punct de vedere legal, tehnic, organizatoric etc.) și de alte condiții interne și/sau externe. Detectarea poate fi proactivă sau reactivă. Detectarea proactivă este procesul descoperirii unor activități suspecte/ neobișnuite, care să ofere indicații privind posibilitatea producerii incidentelor, înainte ca acestea să afecteze resurse ale organizației. Detectarea reactivă este procesul descoperirii unor evenimente ce au afectat deja funcționarea echipamentelor, sistemelor.

Pot exista situații în care activitățile de detectare a incidentelor și vulnerabilităților în rețelele de comunicații electronice sunt realizate de către părți externe.

Organizația trebuie să dețină capabilități de detectare, dar și de prevenire a incidentelor și vulnerabilităților. Pe lângă colectarea informațiilor despre apariția unor incidente și vulnerabilități din diverse surse (din partea personalului, din partea unor părți externe), organizația trebuie să utilizeze instrumente tehnice specifice care să le permită detectarea facilă, în timp util, a incidentelor ce pot afecta securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

1. Sistem de detectare a incidentelor

Este necesar ca organizația să dețină instrumente pentru detectarea reactivă a incidentelor.

Există mai multe surse de detectare reactivă. Astfel:

- personalul care utilizează resursele organizației (echipamente de rețea direct implicate în furnizarea de rețele și/sau servicii de comunicații electronice, elemente ale infrastructurii asociate etc.) poate observa o activitate neobișnuită/suspectă a sistemelor/rețelei/serviciilor pe care o raportează personalului responsabil cu primirea evenimentelor, incidentelor sau vulnerabilităților;

- alte persoane/organizații externe ce desfășoară activități în domeniul securității și integrității rețelelor și serviciilor de comunicații electronice pot transmite organizației alerte sau notificări ce pot conduce la identificarea unor evenimente în cadrul propriei rețele; ulterior procesului de evaluare/triere și decizie acestea pot fi încadrate ca fiind incidente ce pot afecta securitatea și integritatea rețelelor și serviciilor de comunicații electronice;

- utilizatorii serviciilor de comunicații electronice pot transmite informări și sesizări furnizorilor în urma observării unor evenimente ce afectează procesul furnizării rețelelor sau serviciilor de comunicații electronice;

- echipamentele și sistemele din cadrul rețelei pot fi o sursă importantă de detectare a incidentelor și vulnerabilităților prin intermediul alertelor și notificărilor ce pot fi transmise automat.

Astfel, organizația monitorizează în mod continuu sursele precizate anterior în vederea detectării incidentelor și vulnerabilităților.

Evenimentele, incidentele și vulnerabilitățile detectate din diverse surse pot fi corelate. Totodată, este util ca sistemul de detectare a incidentelor să aibă capabilități de corelare a evenimentelor provenind din diverse surse. De exemplu, trebuie să se poată realiza o corelare a sesizărilor primite din partea utilizatorilor de rețele și servicii de comunicații electronice cu evenimentele detectate automat de sistemele dedicate.

1.1 Primirea sesizărilor și notificărilor despre evenimente din partea unor persoane

Evenimentele sau incidentele ce afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice pot fi detectate pe baza primirii unor sesizări sau notificări din partea unor persoane sau organizații. În primul rând astfel de evenimente sau incidente pot fi semnalate de personalul organizației. Informațiile pot proveni și de la părți externe cum sunt de exemplu organizațiile de profil sau alți furnizori de rețele și servicii de comunicații electronice. O altă sursă de detectare o reprezintă informațiile sau sesizările transmise de utilizatorii de rețele și servicii de comunicații electronice.

1.1.1 Informații din partea personalului organizației

Incidentele și vulnerabilitățile pot fi semnalate de personalul organizației (utilizatori ai sistemelor, administratori ai sistemelor/rețelelor, personal de securitate etc.). Așadar, trebuie colectate informații din partea personalului organizației în vederea detectării evenimentelor, incidentelor sau vulnerabilităților.

În cazul observării unui eveniment/incident de securitate sau a unei vulnerabilități este necesară notarea/înregistrarea imediată a tuturor detaliilor importante (de exemplu tipul de neconformitate, încălcare sau disfuncționalitate observată, mesaje apărute pe ecran, informații privind comportamentul neobișnuit al sistemelor/rețelelor/serviciilor).

Evenimentele, incidentele sau vulnerabilitățile pot fi notificate intern prin intermediul unor mijloace de comunicare prestabilite, indiferent de natura acesteia (de exemplu prin comunicare directă, e-mail, fax, telefon, folosind platforme de *ticketing*, prin informarea *NOC*-ului).

Procesele și procedurile asociate detectării și raportării interne au fost abordate în capitolele dedicate.

1.1.2 Informații din partea unor părți externe

Trebuie luate în considerare informații privind incidente și vulnerabilități venite din partea unor părți externe. Aceste informații pot veni de exemplu de la furnizorii de servicii de securitate informatică, alți furnizori de rețele și servicii de comunicații electronice, autorități publice competente, utilizatori de servicii de comunicații electronice.

În vederea colectării informațiilor din partea unor părți externe ce ar putea indica apariția unor evenimente, incidente sau vulnerabilități, organizația trebuie să aibă mecanisme care să permită părților externe notificarea acestora (de exemplu stabilirea unor adrese de e-mail, a unor numere de telefon sau amplasarea unor sisteme de *ticketing* pentru primirea unor astfel de notificări). Astfel de mecanisme vor permite transmiterea mesajelor personalului adecvat. Organizația va monitoriza atent astfel de mecanisme.

1.1.2.1 Sesizări din partea utilizatorilor de servicii de comunicații electronice

Unele evenimente, incidente sau vulnerabilități care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice pot fi detectate pe baza sesizărilor primite din partea

utilizatorilor serviciilor de comunicații electronice (prin informări sau plângeri adresate direct furnizorilor, prin intermediul serviciului de relații cu clienții etc.).

În funcție de capabilitățile de care dispun furnizorii, utilizatorii de rețele și servicii de comunicații electronice pot semnala evenimente, incidente sau vulnerabilități telefonic (prin intermediul serviciului de relații cu clienții – *call center* etc.), prin e-mail, prin fax, poștă, mediul online (de exemplu prin intermediul rețelelor de socializare).

În cadrul actelor normative emise, ANCOM a stabilit în sarcina furnizorilor de servicii de comunicații electronice destinate publicului și obligații în ceea ce privește soluționarea reclamațiilor primite de la utilizatorii finali.

Astfel, Decizia nr. 158/2015 privind obligațiile de informare a utilizatorilor finali[22] prevede în sarcina furnizorilor de servicii de telefonie destinate publicului obligația de a pune la dispoziția publicului „Procedura privind soluționarea reclamațiilor utilizatorilor finali".

De asemenea, prin Decizia nr. 1201/2011 privind stabilirea indicatorilor de calitate pentru furnizarea serviciului de acces la internet și publicarea parametrilor aferenți[23], ANCOM a stabilit o serie de indicatori administrativi pentru furnizarea serviciului de acces la internet, printre care se regăsesc și cei referitori la deranjamente și reclamații: termenul de remediere a deranjamentelor, frecvența reclamațiilor utilizatorului final, frecvența reclamațiilor referitoare la deranjamente, termenul de soluționare a reclamațiilor primite de la utilizatorii finali. Totodată, ANCOM a stabilit mai multe obligații în sarcina furnizorilor de servicii de acces la internet referitoare la acești indicatori. În vederea monitorizării parametrilor de calitate ai serviciului de acces la internet, furnizorii au obligația de a întocmi și de a actualiza permanent un registru în care vor fi înscrise toate reclamațiile primite de la utilizatorii finali.

1.2 Sisteme de monitorizare automată

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

1.2.1 Monitorizarea rețelelor și serviciilor de comunicații electronice

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

Monitorizarea elementelor rețelei de comunicații electronice se poate realiza de către personalul organizației sau/și de terțe părți agreate.

Păstrarea și îmbunătățirea securității organizației implică monitorizarea și supravegherea tuturor resurselor sale în vederea detectării evenimentelor, incidentelor și vulnerabilităților ce pot afecta acest proces și a diminuării riscului de apariție a incidentelor. Monitorizarea poate prezenta particularități diferite în funcție de funcționalitățile sau caracteristicile tehnice ale elementelor de rețea ce trebuie monitorizate, de locația acestora (fizică și logică) în cadrul arhitecturii rețelei de comunicații electronice etc..

Monitorizarea rețelei de comunicații electronice și detectarea incidentelor și vulnerabilităților se pot face:

[22] Decizia nr. 158/2015 privind obligațiile de informare a utilizatorilor finali se găsește la adresa http://www.ancom.org.ro/uploads/forms_files/decizia_2015_1581428306401.pdf

[23] Decizia nr. 1201/2011 privind stabilirea indicatorilor de calitate pentru furnizarea serviciului de acces la internet și publicarea parametrilor aferenți se găsește la adresa http://www.ancom.org.ro/uploads/forms_files/decizie_2011_12011322490368.pdf

- la nivel de rețea în ansamblul său;

- pe baza divizării rețelei în mai multe segmente în funcție de funcționalitățile elementelor sale;

- la nivel de echipamente distincte;

- la nivel de aplicații distincte.

O listă a categoriilor de resurse și echipamente ce pot fi monitorizate se regăsește la capitolul 3.1.2 Evaluare/triere și decizie. În plus, furnizorii pot monitoriza funcționarea echipamentelor instalate la client (*CPE*) și a aplicațiilor, bazelor de date, serviciilor asociate, precum și a altor echipamente și sisteme ce susțin procesul furnizării rețelelor și serviciilor de comunicații electronice.

Unele elemente de rețea critice, a căror defectare poate afecta în mod semnificativ furnizarea rețelelor și serviciilor de comunicații electronice, pot necesita o monitorizare suplimentară, mai strictă.

În funcție de tipul echipamentului, rolul în cadrul rețelei de comunicații, posibilitățile sau limitările tehnice ale acestuia, monitorizarea se poate realiza local sau la distanță (*remote*).

Pentru detectarea evenimentelor, incidentelor și vulnerabilităților, trebuie stabiliți parametri și praguri predefinite la atingerea cărora sistemul de monitorizare să genereze alerte, notificări și rapoarte specifice ce vor fi trimise echipei de răspuns la incidente.

Supravegherea alarmelor privind funcționarea rețelei de comunicații are un rol important în managementul rețelei de comunicații și se referă la acea componentă a sistemului de monitorizare ce vizează detectarea defecțiunilor – *faults* (aproape) în timp real. Funcțiile supravegherii alarmelor sunt folosite pentru monitorizarea și interogarea elementelor de rețea despre disfuncționalități, defecțiuni, anomalii. Managementul alarmelor cuprinde recepționarea, procesarea și afișarea alarmelor de la elementele de rețea. *TMN*[24] specifică diferite nivele de alarmă: alarmă critică, majoră, minoră și de atenționare.

Sistemele și echipamentele de rețea (servere, routere, switch-uri, firewall-uri, servere proxy, VPN-uri, IDS-uri etc.), sistemele de operare, serviciile și aplicațiile generează **log-uri** ce conțin informații privind activitățile desfășurate în cadrul rețelei și pot reprezenta o sursă de detectare a erorilor, disfuncționalităților, anomaliilor. Log-urile sunt de obicei fișiere text ce permit analiza activității software-ului și generarea de alerte automate și de statistici privind funcționarea echipamentului în cauză.

Analiza acestor log-uri poate oferi informații despre:

- evenimentele care descriu starea unui proces ca fiind parte a unei operații normale (informare);

- erorile apărute care descriu anumite probleme ale proceselor din cadrul sistemelor și dispozitivelor de rețea;

- evenimentele ce anunță posibila deteriorare/degradare a unui serviciu (avertizare);

- evenimentele generate la pierderea funcționalităților anumitor componente (nivel critic);

- evenimente generate de consumul resurselor aferente;

- identificarea codurilor cu potențial dăunător și a semnăturilor de atac.

Organizația trebuie să aibă prevăzut cel puțin un nivel de bază pentru înregistrarea și păstrarea log-urilor sistemelor. Se recomandă un nivel avansat pentru sistemele critice a căror defectare poate afecta în mod semnificativ furnizarea rețelelor și serviciilor de comunicații electronice.

În vederea monitorizării rețelei și serviciilor de comunicații electronice, furnizorii pot utiliza **sisteme, platforme și aplicații specifice**, dedicate. În funcție de capabilitățile de care dispune

[24] *Telecommunications Management Network*

organizația, soluțiile de monitorizare pot fi achiziționate de la diferiți producători sau pot fi dezvoltate intern.

Printre sistemele de monitorizare a rețelelor și de detectare a incidentelor și vulnerabilităților se regăsesc următoarele:

- sisteme de monitorizare și alertare pentru rețele, servicii, echipamente, aplicații (de exemplu sisteme de monitorizare a echipamentelor active de rețea de acces și de backbone, aplicații interne de tip *OSS*[25], *NMS*[26], *EMS*[27], instrumente de monitorizare a performanței rețelei, aplicații de măsurare a traficului de rețea, sisteme de monitorizare a platformelor specifice diferitelor tehnologii, sisteme de monitorizare a fibrei optice și a echipamentelor pentru transport radio etc.);

- senzori, roboți;

- sisteme de securitate: sisteme de detectare a atacurilor de tip *DDoS*, *IDS/IPS/IDPS, Firewalls/Security Gateways, Web Application Firewalls, Honeypots, Network Management Tools, Security Information Management (SIM) tools/Security Event Management (SEM) tools/Security Information and Event Management (SIEM) tools, Antivirus/Antispam/Content Protection Tools, File Integrity Checkers, System logs, Application logs, Database logs, Router logs, Proxy logs, NetFlow, Passive DNS monitoring, Vulnerability Assessment Tools* (a se vedea și Anexa nr.2 la Ghid, unde sunt prezentate câteva astfel de sisteme/soluții);

- sisteme de monitorizare a încărcării rețelei, a capacității de procesare a echipamentelor;

- sisteme de monitorizare/control al accesului fizic la *data centere, site-uri* etc. (a se vedea și capitolul 1.2.3 Monitorizarea accesului în locații);

- sisteme auxiliare (pentru monitorizarea funcționării *UPS*-urilor și alarmare în cazul lipsei tensiunii de alimentare a acestor sisteme, de climatizare, pentru stingerea incendiilor, monitorizarea temperaturii și/sau umidității etc. – a se vedea și capitolul 1.2.4 Monitorizarea mediului).

În vederea unei monitorizări de ansamblu, eficiente, rezultatele monitorizării elementelor componente ale sistemului, cât și a părților distinctive, trebuie **corelate** corespunzător. Corelarea va ține cont de monitorizarea sistemelor și echipamentelor atât din punct de vedere fizic, cât și din punct de vedere logic (a se vedea și capitolele 3.1.2 Evaluare/triere și decizie - din prima parte a Ghidului, 1.2.3 Monitorizarea accesului în locații și 1.2.4 Monitorizarea mediului - din a doua parte a Ghidului).

Astfel, se recomandă integrarea tuturor soluțiilor dedicate de monitorizare într-o singură soluție centralizată. Printre funcțiile unei soluții de monitorizare centralizate a rețelei de comunicații se pot enumera:

- permite vizualizarea continuă a stării rețelei prin detectarea în timp real a defecțiunilor, comportamentelor anormale sau altor evenimente sau incidente ale componentelor rețelei/ sistemelor/aplicațiilor etc.;

- generează și stochează log-uri și alarme în funcție de evenimentele detectate;

- permite crearea unor reguli pe baza cărora se generează alarmele;

- trimite alerte și notificări despre evenimente în timp real;

- permite păstrarea log-urilor perioade îndelungate;

- permite monitorizarea centralizată a echipamentelor sau sistemelor implicate;

- are abilitatea creării corelărilor între rezultate;

- este flexibilă, scalabilă în privința resuselor monitorizate.

Printre soluțiile centralizate de monitorizare, se regăsesc așa numitele sisteme de tip "umbrelă", sisteme de tip *OSS* sau *NMS*. În cadrul organizațiilor de dimensiune mare, soluțiile centralizate de monitorizare pot fi operate de Centrul de Operațiuni de Rețea (*NOC*).

[25] *Operations Support System*
[26] *Network Monitoring System*
[27] *Element Management System*

1.2.1.1 Centrul de Operațiuni de Rețea (*NOC*)

Monitorizarea rețelei de comunicații electronice în vederea detectării evenimentelor, incidentelor și vulnerabilităților ce afectează procesul furnizării rețelelor și serviciilor de comunicații electronice este o atribuție importantă în sfera de activitate a unui *NOC*.

Printre activitățile principale ale unui NOC în ceea ce privește managementul incidentelor, inclusiv din punct de vedere al monitorizării rețelei de comunicații electronice și a infrastructurii asociate, se numără:

- operarea și întreținerea platformelor specifice;

- monitorizarea permanentă a rețelei și serviciilor de comunicații electronice (folosind aplicații sau platforme specifice) prin:

  - identificarea tendințelor traficului sau a încărcării nodurilor;
  - investigații ale echipamentelor;
  - detectarea, analiza și urmărirea alarmelor prin sistemele de management;
  - detectarea evenimentelor, incidentelor și vulnerabilităților din rețea și diagnosticarea acestora prin investigarea cauzelor;
  - monitorizarea sistemelor ce asigură alimentarea electrică;

- efectuarea diagnozei incidentului;

- evaluarea impactului evenimentelor asupra eventualelor servicii afectate;

- aplicarea unor soluții temporare sau finale în vederea restaurării serviciilor;

- remedierea incidentului, inclusiv cu posibile intervenții în teren sau cu suport din partea altor părți;

- notificarea internă a evenimentelor, incidentelor și vulnerabilităților prin sistemul de *ticketing* și escaladerea rezolvării către departamentul specializat - tehnic, IT etc. (de exemplu notificarea departamentelor de suport prin deschiderea de tichete ce sunt aduse la cunoștința celor vizați prin SMS, e-mail și telefonic);

- urmărirea modului de rezolvare până la închiderea incidentului cu consemnarea etapelor urmate;

- comunicarea problemelor către alte părți interesate;

- managementul modificărilor în rețeaua de comunicații;

- documentare în privința incidentului (întocmirea raportului incidentului);

- propuneri pentru prevenirea incidentelor similare.

1.2.2 Monitorizarea rețelei interne

Elementele rețelei interne și resursele informatice aferente, precum baze de date, aplicații, sisteme de operare, trebuie de asemenea monitorizate.

Măsurile aplicate rețelei de comunicații electronice descrise anterior se pot aplica și rețelei interne a organizației. Suplimentar, pot exista sisteme specifice dedicate protecției rețelei interne.

Pentru monitorizarea rețelei interne și resurselor informatice pot fi utilizate soluții de monitorizare specifice (de exemplu aplicații software dedicate cu alertare în cazul incidentelor, soluții integrate de monitorizare, *gateway* prin care este administrată rețeaua internă, software de management dedicat).

1.2.3 Monitorizarea accesului în locații

Organizația trebuie să dețină sisteme de detectare a incidentelor cauzate de accesul neautorizat în:

- zonele/clădirile/centrele de comunicații ce aparțin organizației (de exemplu centrele de comutație, centrele de control și operare, centrele de date);

- încăperile (camerele cu echipamente ale rețelei de comunicații, birouri etc.);

- zonele de operare izolate (de exemplu cabinetele stradale, shelterele/containerele, tablourile de distribuție, pilonii).

Printre sistemele de detectare a incidentelor cauzate de accesul neautorizat în interiorul zonelor/clădirilor/centrelor de comunicații se regăsesc:

- sisteme de supraveghere (camere de supraveghere, de exemplu de tip *CCTV*[28], supraveghere electronică cu senzori de prezență etc.);

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

- sisteme de control acces sau antiefracție cu ajutorul cărora să se poată descoperi accesul neautorizat - detectare reactivă sau tentativele de acces neautorizat - detectare proactivă (de exemplu pe bază de cartele, turnicheți, sisteme de încuietori specifice, sisteme bazate pe senzori, sisteme de avertizare sonoră, de monitorizare cu alarmă).

Este necesară instalarea unor sisteme adecvate de detectare a intruziunilor în interiorul încăperilor. Se recomandă ca aceste încăperi să fie prevăzute cu sisteme de supraveghere adecvate.

Totodată, se recomandă ca echipamentele rețelei de comunicații electronice să fie prevăzute cu sisteme de detectare împotriva accesului fizic neautorizat, inclusiv cele situate în alte locații unde se regăsesc resurse ale organizației (zone izolate unde sunt amplasate sheltere, locații de tip outdoor, magazine din rețeaua de vânzări directe, sedii administrative).

Nu în ultimul rând, trebuie asigurată securitatea locațiilor unde se desfășoară acțiuni de răspuns la incidente.

1.2.4 Monitorizarea mediului

Pentru a reduce efectele dezastruoase ale apariției unor incidente severe (cauzate de incendii, inundații, cutremure, explozii și alte forme de dezastre naturale sau provocate de oameni), organizația trebuie să utilizeze sisteme de detectare, alarmare și alertare adecvate, eficiente (de exemplu sisteme de detecție automată a focului și fumului în încăperi, cu precădere în camerele cu echipamente).

De asemenea, se recomandă ca furnizorii să urmărească condițiile meteorologice pentru a preveni incidentele datorate fenomenelor naturale. Se recomandă utilizarea unor sisteme de tip „avertizare timpurie”.

Echipamentele conexe sau auxiliare care permit funcționarea rețelelor de comunicații electronice vor fi monitorizate corespunzător (de exemplu monitorizarea prezenței energiei electrice/*UPS*-uri, monitorizarea temperaturii site-urilor). Condițiile de mediu, precum temperatura și umiditatea trebuie monitorizate, întrucât pot afecta funcționarea în condiții normale a serviciilor și rețelelor de comunicații electronice.

Echipamentele pot fi monitorizate de la distanță pentru verificarea integrității și disponibilității acestora, pentru detectarea incidentelor și a condițiilor de mediu.

[28] Circuit Closed Television

1.3 Detectare proactivă

Se recomandă ca, în funcție de rezultatele analizei de risc și de direcțiile asumate prin politica de securitate, organizația să dețină sisteme pentru detectarea proactivă a evenimentelor, incidentelor și vulnerabilităților în completarea sistemelor reactive.

Detectarea proactivă se referă în principiu la monitorizarea rețelei prin utilizarea unor instrumente concepute în acest sens. Acest tip de detectare poate presupune acțiuni proactive ale personalului organizației pentru identificarea activităților neobișnuite. Monitorizarea rețelei și a sistemelor asociate se poate realiza de exemplu prin intermediul analizei log-urilor, indicatorilor de trafic etc.. Detectarea proactivă poate include și urmărirea dezvoltării tehnologiei sau monitorizarea publică. Acestea se pot referi la articole, studii, rapoarte etc. disponibile ce pot indica noi vulnerabilități, tipuri noi de atacuri și amenințări, recomandări, soluții sau alte informații relevante ce pot contribui la prevenirea unor incidente. Unele părți externe pot pune la dispoziție sau publica informații privind noi vulnerabilități (exploatate sau nu) și amenințări ce pot sprijini detectarea proactivă în cadrul organizației. Un exemplu în acest sens poate fi o organizație din domeniul securității informatice/cibernetice ce pune la dispoziție informații privind infiltrarea și propagarea unui virus sau unui malware într-o anumită regiune geografică, pe anumite sisteme, tehnologii sau terminale.

Log-urile și indicatorii de trafic pot fi utilizați atât pentru investigarea unui incident (acțiuni reactive), cât și pentru identificarea unor activități neobișnuite ce pot indica posibile evenimente, incidente sau vulnerabilități (acțiuni proactive).

2. Evaluarea și actualizarea sistemului de detectare

Sistemul de detectare a incidentelor trebuie evaluat și actualizat periodic, însă cel puțin o dată pe an.

Evaluarea și actualizarea trebuie să cuprindă toate sistemele asociate detectării și raportării incidentelor și vulnerabilităților.

Actualizarea sistemelor poate ține cont de schimbările înregistrate în cadrul rețelei (de exemplu necesitatea măririi ariei de detectare a incidentelor și vulnerabilităților ca urmare a unor modificări ale arhitecturii rețelei de comunicații datorate introducerii unor noi tehnologii sau echipamente), de modificările asupra proceselor afacerii și de incidentele petrecute (de exemplu necesitatea adăugării unor funcții suplimentare pentru detectarea unor noi tipuri de evenimente sau vulnerabilități).

Sistemele pentru detectarea incidentelor pot fi evaluate pe baza unor criterii precum:

- promptitudinea detectării (se referă la intervalul de timp între observarea evenimentului și transmiterea informațiilor sau a alertelor);

- acuratețea detectării (descrie calitatea informațiilor furnizate de către sistem);

- ușurința utilizării (descrie cât de ușor se poate accesa și utiliza informația furnizată de sistem);

- acoperirea (se referă la trei aspecte: partea de rețea monitorizată de sistem, infrastructura folosită pentru monitorizare – de exemplu unul sau mai mulți senzori utilizați, varietatea de incidente pe care le poate detecta);

- resursele implicate (descrie impactul implementării din punct de vedere financiar, tehnic, al resurselor umane implicate etc.);

- scalabilitatea (caracterizează abilitatea sistemului de a face față creșterii volumului de date, respectiv măririi capacității sau a dimensiunii rețelei);

- extensibilitatea (definește abilitatea sistemului de a-și extinde funcționalitățile – dezvoltarea unor module suplimentare, a unor soluții software adaptate necesităților etc.).

Aceste criterii, împreună cu alți factori proprii organizației (profilul organizației, rezultatele evaluării riscurilor) contribuie la evaluarea sistemelor de detectare a incidentelor din cadrul organizației și stabilirea adecvării acestora cu cerințele organizației.

III. Proceduri și planuri de comunicare

Conform prevederilor punctului 3 din secțiunea „V. Managementul incidentelor" din Anexa nr.1 la Decizia nr.512/2013, furnizorii au obligația să stabilească o procedură adecvată de raportare a incidentelor către ANCOM, precum și către alte autorități responsabile și să stabilească planuri de comunicare a incidentelor către alte părți externe (furnizori de rețele și servicii de comunicații electronice afectați, media, clienți, parteneri de afaceri etc.).

În cadrul organizației trebuie să existe un proces fluent și eficient de comunicare a informațiilor despre incidente unor părți externe. Acest proces va fi susținut de proceduri și/sau planuri de comunicare care vor fi elaborate ținându-se cont de principii ale comunicării precum transparența, coerența, obiectivitatea.

Totodată, în elaborarea acestora se vor considera aspecte precum:

- scopul/obiectivul comunicării;

- adaptarea comunicării la necesitățile de informare;

- utilizarea de sisteme și modalități de informare eficiente;

- caracterul flexibil al comunicării (de exemplu pentru a putea integra comunicarea informală).

Se recomandă desemnarea unor persoane din interiorul organizației cu roluri în comunicarea externă a informațiilor despre incidente. Planurile și procedurile privind comunicarea informațiilor despre incidente pot diferi în funcție de părțile care trebuie notificate în privința incidentelor.

De regulă, planurile și procedurile de comunicare răspund la întrebări precum cine, cui, ce, când, cum și de ce. Astfel, în funcție de specificul receptorilor, acestea vor stabili:

- părțile interne care transmit mesajele;

- părțile externe care le recepționează;

- ce mesaj va fi transmis și ce tipuri de informații vor fi comunicate;

- momentele de timp când este necesară comunicarea;

- ce modalități, instrumente și canale de comunicare vor fi utilizate;

- motivul/justificarea comunicării.

Pot exista informații ce trebuie comunicate periodic și informații ce trebuie comunicate în funcție de necesitățile și solicitările care apar, pe aspecte punctuale.

Comunicarea informațiilor privind incidentele înregistrate în cadrul organizației se va realiza în conformitate cu politica organizației privind diseminarea informațiilor.

Atunci când se intenționează diseminarea informațiilor despre incidente, trebuie să se țină cont de aspecte legate de securitatea și de confidențialitatea informațiilor.

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

Conform Deciziei nr.512/2013, incidentele ce trebuie raportate Autorității sunt incidentele cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice (definite ca fiind incidentele care afectează cel puțin 5.000 de conexiuni, timp de cel puțin 60 de

minute). Astfel, furnizorii de rețele și servicii de comunicații electronice cu peste 5.000 de conexiuni vor stabili proceduri de raportare a incidentelor către ANCOM.

Decizia prevede în sarcina furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului obligația de a transmite ANCOM o notificare privind existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice.

Astfel, aceștia trebuie să transmită ANCOM:

a) o notificare inițială privind existența/apariția unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice până cel târziu la ora 13:00 a zilei lucrătoare următoare celei în care a fost detectat incidentul, prin e-mail;

b) o notificare finală privind existența unui incident cu impact semnificativ asupra furnizării rețelelor și serviciilor în termen de două săptămâni de la detectarea acestuia, completând un formular tip de raportare, disponibil online.

Pentru transmiterea corectă, completă, precum și pentru armonizarea și păstrarea consecvenței notificărilor transmise, se recomandă automatizarea procesului de colectare a informațiilor despre incidentele ce trebuie raportate către ANCOM, cu respectarea cerințelor de raportare specificate în Decizia nr.512/2013, respectiv prin cuprinderea tuturor informațiilor solicitate în cadrul art.4 (3), în formularul de raportare din Anexa nr.2, luând în considerare instrucțiunile de completare a formularului din Anexa nr.3 la decizia menționată.

Totodată, pentru transmiterea notificărilor privind existența unui incident cu impact semnificativ asupra securității și integrității rețelelor și serviciilor de comunicații electronice, furnizorii pot consulta și Ghidul de raportare a incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice, disponibil pe pagina web a Autorității[29].

Trebuie acordată atenție informațiilor ce trebuie transmise, precum și termenelor de transmitere a notificărilor, impuse de Autoritate. Astfel, se vor stabili reguli privind strângerea în timp util a informațiilor necesare și raportarea către ANCOM conform prevederilor legale în vigoare. Regulile se vor referi la fluxul intern de lucru ce trebuie urmat în vederea colectării și transmiterii în timp util a celor două tipuri de notificări, inclusiv din punct de vedere al instrumentelor interne utilizate.

Se recomandă întocmirea unei diagrame care să prezinte schematic fluxul intern de lucru pentru raportarea incidentelor către ANCOM. Pentru fiecare activitate a fluxului de lucru se pot menționa persoanele responsabile de realizarea sa.

Conform prevederilor legale, organizația trebuie să desemneze persoane de contact pentru raportarea incidentelor către ANCOM.

Furnizorii vor stabili proceduri pentru raportarea incidentelor către ANCOM, dar și către alte autorități responsabile. Procedurile privind comunicarea informațiilor despre incidente vor acoperi toate actele normative aplicabile, dar și alte situații ce pot indica necesitatea comunicării unor informații despre incidente autorităților responsabile.

În funcție de specificul receptorilor (autorităților responsabile), procedurile pot conține:

- aspecte ce pot justifica comunicarea informațiilor despre incidente autorităților responsabile;

- informații privind conținutul comunicărilor;

- instrumentele și modalitățile de comunicare ce pot fi utilizate;

- rolurile și responsabilitățile privind comunicarea incidentelor, inclusiv alocarea acestora personalului corespunzător;

- modul de colectare a informațiilor;

[29] Ghidul de raportare a incidentelor cu impact semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice este disponibil pe site-ul ANCOM, la adresa: http://www.ancom.org.ro/uploads/links_files/20141219_GHID_DE_RAPORTARE_A_INCIDENTELOR.pdf

- aspecte privind evidența comunicărilor transmise etc.

Procedurile vor cuprinde motivația comunicării informațiilor despre incidente (baza legală a comunicării etc.). Este important de stabilit o serie de caracteristici ale informațiilor ce trebuie transmise, de exemplu tipul incidentelor ce trebuie comunicate. Complexitatea informațiilor și formatul de transmitere a acestora contribuie la definirea procedurilor de raportare. Este necesară alocarea de roluri și responsabilități atât pentru persoanele ce vor transmite informațiile, cât și pentru cele ce vor colecta aceste informații. În acest sens, se recomandă ca procedurile să cuprindă îndrumări privind modul de colectare a informațiilor ce urmează a fi transmise. Pentru eficientizarea procesului de comunicare, se recomandă automatizarea colectării informațiilor ce trebuie comunicate. Acestea pot proveni de la mai multe surse din cadrul organizației, de la personal specializat în diverse domenii. Personalul desemnat pentru transmiterea informațiilor va centraliza informațiile în timp util. Un factor important al comunicării este reprezentat de modalitatea de comunicare utilizată. Dacă în actele normative aplicabile nu sunt clar prevăzute mijloacele de comunicare, se recomandă stabilirea lor de comun acord cu părțile implicate.

Procedurile pot include după caz formulare specifice comunicării informațiilor despre incidente grupurilor țintă dedicate. Aceste formulare vor fi în acord cu cerințele legislative și cu necesitățile de informare.

Procedurile de comunicare vor specifica și aspecte legate de păstrarea evidenței comunicărilor transmise. Astfel, se recomandă păstrarea evidenței comunicărilor transmise, care să conțină, în funcție de situație, momentele transmiterii informațiilor, datele de contact ale persoanelor ce au transmis și ale celor care au primit informarea, informațiile transmise, feedback-ul primit etc..

Este necesar ca toate părțile implicate în strângerea și transmiterea informațiilor despre incidente să cunoască aceste proceduri de raportare.

2. Planuri de comunicare către alte părți

În unele cazuri în care incidentul este confirmat, poate fi necesară comunicarea unor informații despre acesta unor părți externe organizației. Necesitatea comunicării poate interveni în cadrul mai multor procese ale schemei de management al incidentelor, de exemplu atunci când apariția incidentului este confirmată, în timpul tratării sale, atunci când este declanșat planul de continuitate a afacerii (când trebuie întreprinse activități de urgență/criză), după închiderea sa, după acțiunile post-incident și deprinderea unor concluzii privind incidentul. Astfel, pe parcursul tratării incidentului, trebuie avute în vedere aspecte legate de comunicarea externă a unor informații despre acesta (ce informații și cui vor fi comunicate, modalitățile de comunicare etc.).

Necesitatea comunicării către diferite părți externe poate veni din interiorul organizației sau din exterior. Este utilă evaluarea necesității, a oportunității și a obligativității comunicării informațiilor despre incidente diferitelor părți externe. Pe baza acestor evaluări, trebuie stabilite planuri de comunicare în privința incidentelor cu respectarea politicilor interne ale organizației, cu părți externe precum mass-media, alți furnizori de rețele și servicii de comunicații electronice, parteneri de afaceri, utilizatori afectați. În vederea unei comunicări eficiente pot fi utile analize privind caracteristicile diferitelor grupuri țintă implicate, care vor determina necesitățile de informare ale fiecărui grup țintă.

Planurile de comunicare răspund nevoilor de informare ale diverselor grupuri țintă.

Comunicarea unor informații către public (utilizatori ai serviciilor de comunicații electronice) este necesară pentru informarea acestuia în privința apariției incidentelor și pentru îndrumările ce pot fi oferite pentru minimizarea efectelor incidentelor. În funcție de impactul incidentului asupra utilizatorilor de rețele și servicii de comunicații electronice, se recomandă informarea acestora imediat după detectare, prin intermediul unor modalități prestabilite în cadrul planurilor de comunicare (de exemplu transmiterea de email-uri directe, SMS-uri, publicarea informațiilor relevante pe pagina proprie de internet). Pentru incidentele majore, pe lângă informarea utilizatorilor în timp util, se recomandă indicarea unor informații de interes precum tipul incidentului, zona geografică afectată, graficul restabilirii serviciului în parametrii normali de funcționare, soluții la îndemâna utilizatorilor pentru micșorarea impactului incidentului.

Totodată, furnizorii trebuie să asigure serviciul de relații cu clienții pentru a veni în sprijinul acestora ori de câte ori informează asupra unor evenimente care afectează securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

Conform Deciziei nr.512/2013, la solicitarea Autorității, furnizorul are obligația de a asigura informarea publicului cu privire la existența unui incident cu impact semnificativ (în sensul definirii din cadrul deciziei), cel puțin prin una dintre următoarele modalități:

- prin intermediul unei secțiuni speciale pe propria pagină de internet;
- prin canalul propriu de televiziune;
- prin intermediul poștei electronice;
- prin intermediul serviciului de mesagerie scurtă;
- prin mass-media.

Este necesar ca mesajele care au în vedere informarea utilizatorilor de servicii de comunicații electronice asupra incidentelor petrecute să fie formulate clar, utilizând un limbaj comun, pentru a fi ușor de înțeles de către cei ce nu sunt familiarizați cu limbajul tehnic, specializat.

Necesitatea comunicării informațiilor privind incidentele petrecute poate viza și alte părți, de exemplu alți furnizori de rețele și servicii de comunicații electronice de pe piața națională de comunicații electronice sau de pe cea din alt stat membru al Uniunii Europene ce sunt sau pot fi afectați de incident, în vederea restrângerii efectelor acestuia. Incidentele de securitate pot depăși granițele organizației, chiar și cele naționale. În cazul unui incident care afectează simultan mai mulți furnizori, colaborarea între furnizori este utilă. Pentru a răspunde unor astfel de incidente, este necesară coordonarea acțiunilor de răspuns și utilizarea informației referitoare la aceste incidente în comun cu organizațiile externe, după caz. Diseminarea informațiilor între furnizori este benefică pentru diminuarea efectelor incidentului, rezolvarea eficientă a acestuia, aplicarea unor lecții învățate în situații similare sau pentru implementarea unor măsuri în scopul prevenirii incidentelor asemănătoare. Anumite informații despre incidente, cum sunt de exemplu cauzele incidentelor, soluțiile de remediere sau măsurile planificate pentru evitarea altor incidente de același tip pot fi de interes pentru alți furnizori.

Informații despre incidentele petrecute ar putea fi transmise partenerilor de afaceri ai furnizorilor de rețele și servicii de comunicații electronice. Aici se pot încadra producători de echipamente și/sau soluții software, organizații în domeniu cu care sunt eventual încheiate protocoale de colaborare etc..

Altă categorie ce ar putea fi interesată de incidentele petrecute este cea reprezentată de mass-media (indiferent de modul de vehiculare a informației utilizat - mijloace scrise sau audio-vizuale).

Pentru categorii precum cele amintite anterior vor fi elaborate planuri de comunicare care să stabilească reguli clare privind informarea vis-a-vis de incidentele petrecute în cadrul organizației.

În funcție de grupurile țintă dedicate și de diversele situații ce pot indica necesitatea comunicării informațiilor despre incidente, planurile de comunicare pot cuprinde:

- rolurile și responsabilitățile privind comunicarea informațiilor despre incidente, inclusiv alocarea acestora personalului corespunzător;
- modalități de comunicare utilizate (informațiile pot fi comunicate prin diferite metode alese în funcție de circumstanțele incidentului - comunicare ad-hoc sau prin intermediul unor formulare care să cuprindă câmpuri aferente în vederea completării tuturor informațiilor ce trebuie comunicate);
- mijloace de comunicare utilizate (poștă, fax, e-mail, site-ul web al organizației, canalul propriu de televiziune, serviciul de mesagerie scurtă, *IVR*-ul, serviciul de relații cu clienții etc.);
- informații privind tipul informațiilor comunicate (tipul incidentelor ce pot fi notificate și criterii în funcție de care se selectează acestea, ce informații trebuie comunicate despre fiecare incident – de exemplu data producerii incidentului, durata de nefuncționare a serviciului sau termenul

estimativ pentru remediere, tipul serviciilor afectate, aria geografică afectată de incident, informații privind apariția unor vulnerabilități de securitate în rețeaua de comunicații electronice, măsurile ce trebuie luate de utilizatori în cazul incidentelor);

- fluxul de lucru ce trebuie urmat în vederea colectării informațiilor necesare;

- aspecte legate de întocmirea și păstrarea evidenței informațiilor/comunicărilor transmise (evidența se poate referi la informații de contact ale diverselor părți externe cărora se transmit în mod uzual informații despre incidente, detalii despre informările transmise, formulare utilizate etc.).

Se recomandă încadrarea planurilor de comunicare în proceduri specifice.

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

Procedurile și planurile de comunicare sau raportare a informațiilor despre incidente trebuie evaluate și actualizate periodic, dar cel puțin o dată pe an.

Se recomandă evaluarea și actualizarea procedurilor de raportare externă a incidentelor ori de câte ori este necesar, în urma modificărilor legislative sau pe baza evaluării rezultatelor și consecințelor raportării incidentelor.

Se pot dezvolta o serie de indicatori de monitorizare și evaluare a procesului de comunicare externă, pentru măsurarea eficienței activităților de informare asupra incidentelor.

Modalități de verificare

Pentru a face dovada stabilirii și implementării unor măsuri adecvate riscului identificat și care respectă obligațiile din cadrul secțiunii *Managementul incidentelor* din Anexa nr.1 la Decizia nr.512/2013, ANCOM poate solicita, separat sau cumulativ:

- prezentarea unor documente (în format fizic sau electronic) relevante, evidențe ale activităților desfășurate în vederea remedierii incidentelor, înregistrări de audit de securitate, evidențe ale testelor de scanare a rețelei și ale verificărilor efectuate în scopul detectării unor amenințări, vulnerabilități, listări ale corespondențelor electronice din care să rezulte implementarea măsurilor respective;

- demonstrarea practică a implementării măsurilor (de exemplu realizarea acțiunilor corespunzătoare proceselor din cadrul schemei de management al incidentelor și aplicarea procedurilor asociate pe anumite scenarii de incidente dezvoltate);

- prezentarea unor instrumente, sisteme și mecanisme implicate în procesul de management al incidentelor;

- organizarea unor interviuri cu persoanele responsabile de implementarea acestor măsuri (de exemplu membri ai echipei de răspuns la incidente).

Printre documentele relevante în vederea demonstrării implementării unor măsuri adecvate în domeniul managementului incidentelor se pot regăsi:

- politica de management al incidentelor;

- proceduri privind managementul incidentelor (care să vizeze procesele de detectare și raportare internă, evaluare, triere și decizie, răspuns și escaladare a incidentelor, colectare a informațiilor despre incidente și păstrarea evidenței acestora);

- documentații actualizate ale sistemului de detectare a incidentelor;

- proceduri și/sau planuri de comunicare a informațiilor despre incidente;

- rapoarte periodice privind incidentele înregistrate în cadrul organizației;

- rapoarte individuale ale incidentelor;

- documente care să ateste înțelegerile contractuale cu alte părți externe relevante din perspectiva managementului incidentelor (dacă este cazul).

Anexa nr.1

Exemple de servicii ce pot fi furnizate de echipa de răspuns la incidente[30]

Servicii reactive

a) alerte și avertizări;

Implică primirea și eventual diseminarea informațiilor ce descriu un incident/o vulnerabilitate (atac informatic, problemă software, lipsă redundanță, malware etc.), însoțite de furnizarea recomandărilor privind soluțiile pe termen scurt pentru gestionarea evenimentului, incidentului sau amenințării, în cazul în care (și) alte persoane dinafara echipei sunt implicate în acțiuni de tratare a incidentului. Echipa de răspuns creează aceste alerte și îndrumări pe baza unor indicatori tehnici sau le redistribuie de la alte părți și le transmite personalului direct implicat în activitățile asociate tratării acestuia. Alertele și avertizările vor fi clasificate în funcție de severitatea incidentelor.

b) gestionarea incidentelor;

Tratarea incidentelor implică primirea, trierea, analiza, răspunsul la evenimente/incidente. Activitățile de tratare a incidentelor pot include:

- luarea unor măsuri pentru protecția sistemelor/rețelelor/serviciilor afectate;

- furnizarea unor soluții și strategii de minimizare a impactului incidentelor;

- inspectarea sistemelor afectate și a celor asociate având în vedere amploarea incidentului pentru a detecta toate intruziunile;

- recuperarea/restabilirea sistemelor/rețelei/serviciilor în parametri normali de funcționare;

- dezvoltarea unor soluții alternative de răspuns.

- analiza incidentelor;

Pot exista mai multe nivele de analiză a unui incident și mai multe subservicii asociate. Analiza înseamnă examinarea tuturor informațiilor disponibile. O analiză eficientă implică existența unui format standard de raportare a evenimentelor, incidentelor sau vulnerabilităților. Scopul analizei îl constituie identificarea categoriei incidentului, amplorii incidentului din punct de vedere al resurselor afectate, opțiunilor de răspuns etc.. Una dintre activitățile implicate în analiza incidentului este determinarea cauzei incidentului. Echipa de răspuns va corela caracteristicile mai multor incidente pentru a identifica tendințe, cauze comune/frecvente etc.

- răspuns „on site" la incidente;

Acest tip de răspuns presupune că echipa de răspuns acționează direct pentru rezolvarea incidentului, fiind prezentă la fața locului. Dacă incidentul nu implică răspunsul direct sau printre responsabilitățile echipei nu se află răspunsul direct, la fața locului incidentului, atunci vor fi desemnate persoane care să se deplaseze la locul incidentului pentru rezolvare (de exemplu o echipă tehnică dedicată pentru intervenția în anumite situații).

- suport pentru răspuns la incidente;

Presupune răspunsul indirect la incidente. Echipa de răspuns nu se va deplasa la locul incidentului și va îndruma de la distanță persoanele desemnate pentru soluționare. Echipa va oferi suportul persoanelor direct implicate prin intermediul diverselor mijloace de comunicare și/sau prin oferirea unor documentații adecvate. Suportul poate implica asistența tehnică în interpretarea informațiilor despre incidente, îndrumări în vederea diminuării impactului și identificării soluțiilor de recuperare.

- coordonarea răspunsului la incidente;

Nu implică răspunsul direct, la fața locului, la incident. Echipa coordonează activitățile de răspuns, printre alte părți implicate. Coordonarea poate presupune colectarea unor informații,

[30] În prezentarea exemplelor s-a ţinut cont de serviciile *CSIRT*, disponibile pe site-ul *ENISA* (Agenţia Europeană pentru Securitatea Reţelelor Informatice şi a Datelor): https://www.enisa.europa.eu/activities/cert/support/guide/appendix/csirt-services

notificarea părților implicate, facilitarea schimbului de informații, colaborarea cu alte compartimente ale organizației (de exemplu juridic, relații publice).

c) gestionarea vulnerabilităților;

Implică primirea informațiilor/notificărilor privind vulnerabilități detectate, analiza naturii, efectelor acestora și dezvoltarea soluțiilor/strategiilor pentru eliminarea lor. În funcție de tipul activităților desfășurate, echipa de răspuns poate acționa pentru:

- analiza vulnerabilităților;

Echipa de răspuns analizează din punct de vedere tehnic (dar nu numai) vulnerabilitățile suspectate, ceea ce implică examinarea acestora în vederea determinării locației acestora în sisteme/rețea, modului în care pot fi exploatate de amenințări etc.. Aceste activități pot fi asociate cu simularea unui incident declanșat prin exploatarea unei vulnerabilități (de exemplu prin utilizarea unui sistem de test).

- răspunsul la vulnerabilități;

Presupune determinarea răspunsului adecvat pentru diminuarea sau anularea vulnerabilităților, ceea ce poate implica dezvoltarea unor soluții de remediere, crearea unor îndrumări/alerte privind soluțiile posibile de remediere etc..

- coordonarea răspunsului la vulnerabilități;

Echipa de răspuns notifică părțile implicate ale organizației în privința vulnerabilităților și le informează în ceea ce privește modalitățile posibile de diminuare/anulare a acestora. De asemenea, echipa de răspuns comunică cu alte părți (de exemplu producători de echipamente și soluții software, alte echipe de răspuns la incidente, experți tehnici în domeniu), verifică implementarea strategiei de răspuns la vulnerabilități, coordonează aplicarea soluțiilor de remediere, sintetizează analiza tehnică realizată de alte părți (dacă este cazul), menține evidența informațiilor despre ciclul de viață al vulnerabilităților etc..

d) gestionarea artefactelor;

Un artefact este orice fișier sau obiect descoperit pe un sistem, care ar putea fi implicat în penetrarea sau atacarea sistemelor și rețelelor. Artefactele pot să includă, dar nu sunt limitate la viruși de calculator, programe de tip cal troian, viermi, script-uri de exploatare și toolkit-uri. Gestionarea artefactelor implică primirea informațiilor despre acestea și copii ale artefactelor care sunt folosite în atacuri ale intrușilor, recunoaștere și alte activități neautorizate sau nocive. Odată recepționat, artefactul este analizat. Acest lucru include analiza naturii, versiunii și utilizării artefactelor și dezvoltarea (sau sugerarea) strategiilor de răspuns pentru detectarea, eliminarea și protecția împotriva acestor artefacte. Deoarece activitățile de gestionare a artefactelor pot fi implementate în diverse moduri, acest serviciu este categorisit mai departe pe baza tipului de activități efectuate și a tipului de asistență acordată, astfel:

- analiza artefactelor;

Echipa de răspuns efectuează o examinare tehnică și o analiză a oricărui artefact găsit pe un sistem. Analiza efectuată ar putea să includă identificarea tipului de fișier și a structurii artefactului, compararea unui artefact nou cu artefactele existente sau alte versiuni ale aceluiași artefact pentru a vedea similitudinile și diferențele, ingineria inversă sau dezasamblarea codului pentru a determina scopul și funcția artefactului.

- răspunsul la artefacte;

Acest serviciu implică determinarea acțiunilor corespunzătoare pentru detectarea și eliminarea artefactelor de pe un sistem, precum și acțiuni de prevenire a instalării artefactelor. Acest lucru poate să implice crearea de semnături care să poată fi adăugate la programele software antivirus sau IDS.

- coordonarea răspunsului la artefacte;

Acest serviciu se referă la comunicarea și sintetizarea rezultatelor de analiză și a strategiilor de răspuns asociate unui artefact cu ajutorul altor experți în securitate. Activitățile includ notificarea

altora și sintetizarea analizelor tehnice dintr-o varietate de surse. Activitățile pot să includă menținerea unei arhive publice sau private cu artefacte cunoscute, impactul acestora și strategiile de răspuns corespunzătoare.

Servicii proactive

a) anunțuri;

Include alerte de intruziuni, avertizări de vulnerabilități, îndrumări în privința securității etc.. Astfel de anunțuri informează părțile implicate cu privire la aspecte ale evoluției/dezvoltării din punct de vedere tehnic a unor sisteme/a rețelei, cu impact asupra securității (de exemplu noi vulnerabilități descoperite) și facilitează protejarea sistemelor și rețelelor împotriva unor vulnerabilități neexploatate încă.

b) urmărirea dezvoltării tehnologiei;

Echipa de răspuns la incidente monitorizează/urmărește evoluția din punct de vedere tehnic a sistemelor/rețelei, precum și activitățile cu potențial malițios pentru a identifica noi amenințări. Implică informarea în domenii ale științei, tehnologiei etc. (urmărirea unor pagini web/articole) pentru a extrage informații relevante în domeniul securității. Rezultatul acestor tipuri de activități îl poate reprezenta elaborarea unor ghiduri privind aspecte de securitate.

c) audituri și evaluări de securitate;

Presupune analiza/revizuirea securității pe baza cerințelor stabilite de organizație, prevederilor legale, standardelor aplicabile etc.. Poate consta în:

- revizuirea infrastructurii (revizuirea configurațiilor hardware, software, routere, firewall-uri, servere etc. pentru a verifica îndeplinirea politicilor de securitate ale organizației și prevederilor legale, normelor, standardelor aplicabile etc.);

- scanarea sistemelor/rețelelor din punct de vedere al virușilor, vulnerabilităților etc. pentru identificarea celor vulnerabile;

- testarea penetrării (testarea securității prin simularea unor atacuri).

Activitățile specifice pot include dezvoltarea unor reguli/proceduri privind circumstanțele/condițiile desfășurării evaluărilor/auditurilor, inclusiv cerințe privind expertiza și instruirea personalului responsabil cu efectuarea acestora. Activitățile pot fi externalizate prin contractarea unor auditori/experți în domeniu.

- analiza celor mai bune practici;

Presupune intervievarea angajaților pentru a stabili dacă practicile lor de securitate se potrivesc cu politica de securitate definită în organizație sau cu unele standarde specifice industriei.

d) configurarea și mentenanța instrumentelor de securitate, aplicațiilor, infrastructurilor și serviciilor;

Pe lângă oferirea unor îndrumări privind modul de configurare, mentenanță al echipamentelor/sistemelor/serviciilor/aplicațiilor de securitate, echipa poate acționa în sensul actualizărilor, mentenanței acestor echipamente/sisteme/servicii/aplicații. Orice probleme legate de vulnerabilitățile unor sisteme în urma configurării/utilizării lor vor fi escaladate personalului responsabil.

e) dezvoltarea instrumentelor de securitate;

Constă în dezvoltarea unor noi dispozitive (tool-uri) necesare echipei de răspuns sau a unor tool-uri ce extind funcționalitățile celor existente.

f) servicii de detectare a intruziunilor;

Echipa revizuiește log-urile sistemelor IDS, analizează și inițiază răspunsul pentru evenimentele ce îndeplinesc pragul stabilit sau direcționează alertele pe baza unor reguli de escaladare stabilite. Colectarea și analiza informațiilor capturate de log-urile IDS-urilor pot presupune un efort semnificativ astfel încât sunt necesare tool-uri și expertiză adecvate pentru sinteza și

interpretarea informațiilor în vederea identificării alarmelor false, atacurilor și altor evenimente petrecute în rețea și implementării unor măsuri pentru reducerea/anularea acestor evenimente. Astfel de activități pot fi externalizate unor persoane/echipe cu expertiză în domeniu.

g) diseminarea informațiilor privind securitatea.

Constă în colectarea și transmiterea părților interesate din organizație a unor informații ce pot ajuta la îmbunătățirea nivelului de securitate. Aceste informații s-ar putea referi la arhive ale alertelor, avertizărilor, documentații ale bunelor practici în domeniu, politici, proceduri, statistici, tendințe etc.. Acestea pot fi corelate cu informații din partea unor părți externe (producători de echipamente sau soluții software, alte echipe de răspuns la incidente, experți în domeniu etc.).

Servicii de management al calității securității

a) analiza riscurilor;

Echipele de răspuns pot contribui la analiza și evaluările riscurilor. Acest lucru poate îmbunătăți capacitatea organizației de a evalua amenințările reale, de a furniza evaluări realiste, calitative și cantitative ale riscurilor și de a evalua strategiile de protecție și răspuns.

b) planuri de continuitate a afacerii și de recuperare în caz de dezastru;

Eforturile de planificare trebuie să ia în considerare experiența și recomandările echipei pentru determinarea celui mai bun mod de a răspunde la astfel de incidente și pentru asigurarea continuității afacerii. Echipele care implementează acest serviciu pot fi implicate în continuitatea afacerii și planificarea recuperării în urma dezastrului în cazul evenimentelor asociate cu amenințările sau atacurile la adresa securității.

c) consultanța privind securitatea;

Echipele pot furniza sfaturi și indicații despre cele mai bune practici de securitate care pot fi implementate. O echipă care furnizează acest serviciu este implicată în pregătirea recomandărilor sau identificarea cerințelor de instalare sau securizare a noilor sisteme, elemente de rețea, aplicații software etc..

d) dezvoltarea gradului de conștientizare;

Echipele pot identifica domeniile ce necesită mai multe informații și indicații pentru o mai bună conformare la practicile de securitate acceptate și politicile de securitate la nivel de organizație. Creșterea gradului general de conștientizare în materie de securitate nu numai că ameliorează înțelegerea problemelor de securitate, dar ajută și la efectuarea operațiunilor zilnice într-o manieră mai sigură. Echipa care efectuează acest serviciu caută oportunități pentru a mări gradul de conștientizare în materie de securitate prin crearea de articole, postere, buletine de știri, site-uri web sau alte resurse informaționale care explică cele mai bune practici de securitate și furnizează sfaturi în legătură cu măsurile de precauție ce pot fi adoptate.

e) instruire;

Acest serviciu implică furnizarea de informații în legătură cu problemele de securitate prin intermediul seminarelor, atelierelor, cursurilor și tutorialelor. Subiectele pot include indicații generale de raportare a incidentelor, metode de răspuns potrivite, instrumente de răspuns la incidente, metode de prevenire a incidentelor și alte informații necesare pentru protejarea, detectarea, raportarea și răspunsul la incidente de securitate.

f) certificare;

Echipa poate realiza evaluări pentru a asigura securitatea și conformitatea cu practici de securitate acceptabile pentru organizație. Instrumentele și aplicațiile analizate pot fi produse open source sau comerciale. Acest serviciu poate fi furnizat ca o evaluare sau printr-un program de certificare, în funcție de standardele aplicate de către organizație.

Sisteme de detectare a incidentelor

a) Application logs

Application logs implică analiza log-urilor de tip *system logs*, *database logs* și *proxy logs*. Monitorizarea și analiza log-urilor pot fi folosite ca parte a unui sistem de avertizare timpurie. Diverse interogări care generează erori sau încercări incorecte de conectare pot fi colectate de la o serie de log-uri.

b) Firewall

Un *firewall* („zid de protecție") joacă un rol semnificativ în procesul de securitate a unei rețele de calculatoare. Firewall-urile sunt de obicei prezente în orice infrastructură de rețea. Firewall-ul este un dispozitiv sau o aplicație concepută pentru a filtra (permite sau interzice) conexiunile de rețea, controlând procesul de comunicație dintre rețeaua internă și cea externă, prin aplicarea politicii de securitate a rețelei protejate. Se recomandă filtrarea și analiza atât a traficului de intrare, cât și a celui de ieșire. Firewall-ul protejează rețeaua privată de atacurile externe și restricționează accesul din afară la resursele acesteia. Întrucât firewall-ul reprezintă singura conexiune dintre rețeaua privată și cea publică, la nivelul său se poate monitoriza și jurnaliza traficul de pachete și se verifică drepturile de acces ale utilizatorilor din afara rețelei interne. Politica de securitate aplicată de firewall stabilește regulile pe baza cărora se admite sau se blochează transferul pachetelor între rețeaua privată și cea publică. Pot fi create alerte direct în cadrul firewall-ului sau se pot utiliza sisteme/dispozitive adiționale pentru analiza log-urilor firewall-ului. Analiza log-urilor poate implica hardware adițional, în funcție de volumul de trafic/amploarea rețelei. De regulă, firewall-urile sunt centrate pe analiza unui volum mare de trafic.

c) IDS/IPS/IDPS

Un *IDS*[31] este o componentă software (adesea integrată cu dispozitivul) care monitorizează și analizează traficul de rețea sau comportamentul sistemului de operare pentru detectarea activităților neautorizate/malițioase. Un *IDS* este așadar un sistem informatic utilizat pentru identificarea unor încercări de intruziuni, intruziuni ce au sau au avut loc și eventual pentru răspunsul la intruziuni în rețele și sisteme informatice. Un sistem *IDS* lucrează de obicei în modul pasiv – detectează amenințări, înregistrează informațiile și declanșează o alertă. Definit ca un instrument de identificare, inventariere și raportare a traficului de rețea neautorizat, un sistem *IDS* reprezintă o soluție alternativă ce permite administratorilor de rețea și de securitate să identifice în timp optim încercările de atac asupra unui sistem informatic. Un sistem *IDS* inspectează toată activitatea rețelei și identifică structuri de date suspecte ce pot indica un atac din partea cuiva care încearcă să se conecteze sau să compromită un sistem. Sistemele de detectare și/sau prevenire a intruziunilor (*IDS/IPS/IDPS*) identifică evenimente suspecte/neobișnuite și înregistrează informații relevante (data și ora detectării evenimentului, tipul său, adresele IP sursă și destinație etc.). *IDS*-ul este software-ul ce automatizează procesul de detectare a intruziunilor.

Un *IPS* este similar cu un *IDS*, dar lucrează de obicei în modul activ – este capabil să blocheze comportamentul malițios. Astfel, *IPS*-ul poate stopa/evita incidente posibile. Sistemele *IDPS* sunt sisteme hibride ce înglobează capacități de detectare și prevenire (*IDS* și *IPS*).

Mecanismele de detectare în sistemele *IDS* și *IPS* sunt clasificate în două mari categorii: bazate pe semnături (activitatea este comparată cu modele de atac predefinite) și bazate pe anomalii (este detectată activitatea anormală a sistemului/rețelei). De regulă, un sistem *IDS* are capacitatea de a acoperi mare parte a rețelei. Sistemele comerciale *IDS* și *IPS* sunt de obicei livrate ca și sisteme hardware, iar cele noncomerciale sunt livrate ca și software, iar hardware-ul trebuie achiziționat separat.

[31] Mai multe informaţii despre implementarea IDS-urilor se găsesc în Standardul Internaţional *ISO/IEC 27039:2015 Information technology - Security techniques - Selection, deployment and operations of intrusion detection systems (IDPS)*[31].

Scopul IDS-urilor este monitorizarea pasivă, detectarea și înregistrarea (*logging*) activităților anormale sau suspecte ce pot reprezenta intruziuni și alertarea atunci când aceste activități sunt detectate. Organizația poate implementa astfel de sisteme prin achiziționarea produselor software și/sau hardware IDS sau prin externalizarea capabilităților IDS-ului către un furnizor de astfel de servicii. Există două tipuri de IDS - *Host-based IDS* (HIDS) și *Network-based IDS* (NIDS) și două abordări de bază pentru analiza intruziunilor detectate – bazată pe identificarea semnăturilor de atac la nivel de aplicație (*Misuse-based approach*) și bazată pe anomaliile de trafic (*Anomaly-based approach*). Pentru a acoperi intruziunile potențiale și pentru o bună analiză a alertelor, se recomandă combinarea celor două tipuri de abordări.

Selectarea unor IDS-uri potrivite necesităților organizației depinde de factori precum:

- evaluarea riscurilor la adresa securității;

Pentru alegerea IDS-urilor potrivite, organizația va evalua riscurile la adresa securității. Astfel vor fi identificate amenințările/vulnerabilitățile sistemelor și va fi posibilă alegerea măsurilor care să asigure reducerea riscurilor.

- alegerea tipurilor de IDS (HIDS și/sau NIDS);

- informații privind:

i. circumstanțele/mediul în care va fi implementat sistemul din punct de vedere al caracteristicilor tehnice (diagrame/hărți ale rețelei care să specifice numărul și locațiile stațiilor, punctele de acces în rețele și conexiunile cu rețelele externe, numărul și tipul echipamentelor de rețea precum routere, switch-uri, bridge-uri, numărul, tipul și descrierea serverelor de rețea etc.);

ii. politica de securitate pentru IDS – în care să se clarifice aspecte precum: sistemele ce vor fi monitorizate, tipul sistemelor IDS necesare, locația amplasării IDS-urilor, tipurile de atacuri/intruziuni ce trebuie detectate, tipul informațiilor ce trebuie înregistrate, tipul de răspuns și alertă necesar/ă la detectarea unor astfel de evenimente;

iii. evaluarea performanței și eficienței IDS-urilor (lățimea de bandă necesară, nivelul de alarme false tolerate etc.);

iv. verificarea capabilităților IDS-urilor (de exemplu prin solicitarea unor informații de la producătorii soluțiilor IDS);

v. analiza costurilor (pot fi implicate costuri de achiziționare a IDS-ului, costuri privind achiziționarea sistemului pe care să ruleze software-ul IDS, asistență specializată în instalarea și configurarea IDS-ului, instruirea personalului, mentenanța sistemului etc.).

- selectarea unor instrumente care să sporească/completeze funcționalitățile IDS;

IDS nu este singura soluție de detectare a intruziunilor și de reducere a impactului acestora. Există instrumente pentru sporirea și completarea capacităților/funcțiilor IDS-urilor precum: *File Integrity Checkers, Firewalls/Security Gateways, Honeypots, Network Management Tools, Virus/Content Protection Tools, Vulnerability Assessment Tools.*

- investigarea scalabilității IDS-urilor;

- evaluarea necesității suportului tehnic.

Se recomandă o abordare etapizată a implementării IDS-urilor, pornind de la NIDS, continuând cu protejarea serverelor critice folosind HIDS.

Locația aleasă pentru NIDS are un rol important în implementarea sistemului, orice locație aleasă prezentând atât avantaje, cât și dezavantaje. NIDS poate fi plasat în interiorul sau în exteriorul unui firewall internet, într-un backbone major al rețelei, în subrețelele critice.

Trebuie avute în vedere măsuri pentru protecția datelor stocate în baza de date IDS, referitoare la activitatea suspectă și la atacurile înregistrate în cadrul organizației. Ca orice alt element de rețea, IDS-ul poate fi vulnerabil la evenimente de securitate, implementarea nesigură a unui senzor IDS poate expune sistemul la atacuri etc..

Serviciile asociate IDS-ului pot fi asigurate de personalul specializat în managementul incidentelor din cadrul organizației (echipa de răspuns la incidente etc.) sau pot fi externalizate unor părți terțe. Sistemele IDS oferă mai multe opțiuni de răspuns, active sau pasive. Răspunsul activ implică o acțiune automată a sistemului în detectarea unui atac. Aceste sisteme sunt de fapt cunoscute sub denumirea IPS. Acțiunile de răspuns ale unui IPS pot fi colectarea unor informații suplimentare privind atacul suspectat, schimbarea mediului sistemului pentru a opri atacul, închiderea sesiunii de comunicații. IPS reprezintă fuziunea capabilităților de protecție cu cele de detectare a intruziunilor, făcând posibilă detectarea unui atac și protecția împotriva acestuia în mod static sau dinamic. IPS asigură protecția resurselor informatice prin eliminarea traficului cu potențial dăunător al rețelei, permițând traficul legitim. Răspunsul activ prezintă avantaje precum detectarea și blocarea atacurilor, asigurarea protecției proactive, creșterea eficienței operaționale. Răspunsul pasiv poate consta în alarme și notificări, ferestre popup, mesaje transmise pe telefoane mobile etc..

IDS-ul este diferit de firewall. Firewall-ul limitează accesul la rețea prevenind intruziunile, dar nu semnalizează atacuri sau conexiuni neautorizate din rețea. Comparativ cu un sistem firewall, care, pe baza politicilor de tip *allow* și a celor de tip *deny* controlează traficul la perimetrul unei rețele, sistemele IDS analizează traficul de date permis de către un firewall sau router pentru identificarea tentativelor de atac.

Sistemele IDS pot fi de regulă sisteme hardware de sine stătătoare ce supraveghează traficul, aplicații software pentru servere dedicate sau module hardware de tip *add-in* pentru firewall-ul existent.

Aceste sisteme detectează atacurile, declașeanză răspunsuri la aceste atacuri și totodată alertează pe diverse căi personalul responsabil (administratorul de rețea, echipa de răspuns la incidente etc.).

Alertarea în cazul unui potențial atac este un serviciu extrem de util pentru administratori, care pot astfel interveni în timp optim pentru protejarea rețelei. Sistemele de tip IDS nu blochează atacul ci doar îl înregistrează pentru o monitorizare ulterioară.

Serviciile de detectare a intruziunilor execută la nivel de dispozitiv de rețea următoarele funcții:

- inspectează fluxul de date care trece prin rețea, identifică semnăturile activităților neautorizate și activează procedurile de apărare;
- generează alarme în cazul detectării evenimentelor, notificând personalul de securitate;
- activează un răspuns automat în cazul anumitor probleme.

Inițiatorii atacurilor pot fi persoane din exteriorul rețelei, persoane autorizate din interior care folosesc incorect privilegiile deținute sau persoane neautorizate din interior care urmăresc obținerea de privilegii ce nu li se cuvin.

Politica de securitate poate defini informațiile ce trebuie protejate, tipul IDS-ului necesar, locația unde va fi instalat, ce tipuri de atacuri va detecta și în funcție de acești parametri, ce tip de alerte sau răspunsuri va fi necesar să ofere atunci când este detectat un atac real. Sistemele IDS pot controla o gamă largă de tipuri de atacuri, inclusiv DoS (*Denial of Service*) sau DDoS (*Distributed Denial of Service*). Sistemele IDS trebuie să monitorizeze atât traficul care intră, cât și pe cel care iese din rețea.

d) NetFlow

NetFlow este un protocol de rețea dedicat colectării, monitorizării și analizei traficului IP în vederea identificării incidentelor potențiale, permițând detectarea proactivă a incidentelor. Acest protocol este utilizat de dispozitivele/elementele active ale rețelei (routere, switchuri) și implică utilizarea unor dispozitive adecvate și a unor sisteme/soluții software pentru analiza și generarea statisticilor pe baza informațiilor colectate. Există soluții similare implementate sub diferite nume precum *jFlow*, *sFlow*, *NetStream*, *nProbe*. *NetFlow* poate fi folosit pentru detectarea anomaliilor și traficului anormal și ajută în special la scanare și în procesul detectării atacurilor *DDoS* și diminuării efectelor/impactului acestora.

e) Security Information Management (SIM) tools/Security Event Management (SEM) tools/Security Information and Event Management (SIEM) tools

SIEM reprezintă acel software de analiză a evenimentelor de securitate și a comportamentelor anormale din rețea ce sunt extrase din jurnalele aplicațiilor, sistemelor și echipamentelor din rețea. *SIEM* implică colectarea, arhivarea, analiza, corelarea și raportarea informațiilor obținute de la toate resursele eterogene ale rețelei. Tehnologia *SIEM* se află la intersecția dintre *SIM* (*Security Information Management*) și *SEM* (*Security Event Management*).

f) Antivirus/Antispam

Programele antivirus pot preveni infectarea sistemelor gazdă, detecta forme de malware/conținut suspicios, genera alerte și elimina software-ul malițios. Teoretic, acestea pot scana tot traficul (de intrare și de ieșire). Software-ul antispam detectează și previne e-mail-urile de tip spam, alertele venite de la acest soft pot indica încercări de atac.

g) Honeypots

Un *honeypot* reprezintă o capcană pentru detectarea și urmărirea încercărilor de utilizare neautorizată a serviciilor rețelei 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 și colectează informațiile privind tendințele atacurilor. Honeypot-urile pot fi plasate în multe locații ale rețelei (fizice și logice). De obicei, honeypot-urile detectează amenințări ce folosesc scanarea pentru propagare: *bots, scanning worms* etc..

h) Sandboxes

Sandbox este un mediu în care un cod suspicios sau o aplicație pot rula izolat fără să afecteze un sistem de operare (mediul acesta este separat de sistemul de operare). Tot comportamentul software-ului analizat este înregistrat incluzându-se conexiunile de rețea. Informația dobândită în procesul de analiză oferă posibilitatea deducerii dacă software-ul este sau nu malițios. Pentru observații la scară largă sunt necesare mai multe mașini ce pot fi asigurate și într-un mediu virtual.

Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii (ANCOM) este instituţia care protejează interesele utilizatorilor de comunicaţii din România, prin promovarea concurenţei pe piaţa de comunicaţii, administrarea resurselor limitate, încurajarea investiţiilor eficiente în infrastructură şi a inovaţiei. Pentru mai multe detalii despre activitatea ANCOM vizitaţi www.ancom.org.ro, www.portabilitate.ro şi www.veritel.ro. Pentru a testa și monitoriza calitatea serviciului de internet, accesați www.netograf.ro.