ANCOM
Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii

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

ANEXA nr. 1 a Deciziei preşedintelui ANCOM nr.512/2013

Domeniile vizate de măsurile minime de securitate

I. Politica de securitate şi managementul riscului

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească o politică de securitate adecvată;

2) să stabilească un management al riscului care:

a) să stabilească domeniul de aplicare, precum şi criteriile de bază necesare procesului de management al riscului (criteriul de evaluare a riscului, criteriul de stabilire a impactului, criteriul de acceptare a riscului);

b) să identifice riscurile, prin identificarea resurselor furnizorului în cauză, ameninţărilor, vulnerabilităţilor, măsurilor existente şi a consecinţelor pe care pierderea/încălcarea securităţii le-ar putea avea asupra resurselor;

c) să estimeze riscurile prin evaluarea impactului pe care îl poate avea concretizarea unei ameninţări care exploatează o vulnerabilitate a unei resurse şi prin evaluarea probabilităţii de apariţie a incidentelor;

d) să evalueze riscul;

e) să evalueze opţiunile de tratare a riscului, să selecteze măsuri pentru tratarea riscului cu fixarea obiectivelor acestor măsuri şi să justifice riscurile acceptate care nu îndeplinesc criteriul de acceptare a riscului.

3) să stabilească o structură adecvată a rolurilor şi responsabilităţilor în asigurarea securităţii şi integrităţii reţelelor şi serviciilor;

4) să stabilească o politică cu privire la cerinţele de securitate pentru achiziţionarea de produse şi servicii de la terţe părţi şi pentru asigurarea întreţinerii sau gestiunii de către terţe părţi a produselor şi serviciilor (servicii IT, software, interconectare, baze de date, facilităţi asociate etc).

II. Securitatea resurselor umane

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să efectueze controale de verificare de fond a candidaţilor pentru angajare, a contractorilor şi a terţilor în conformitate cu legile aplicabile, reglementări şi etică, proporţionale cu riscurile percepute;

2) să se asigure că personalul lor are cunoştinţe suficiente de securitate şi este instruit permanent cu privire la securitatea şi integritatea reţelelor şi serviciilor;

3) să stabilească un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri şi responsabilităţi;

4) să stabilească un proces disciplinar pentru angajaţii care produc o încălcare a securităţii şi integrităţii reţelelor sau serviciilor de comunicaţii electronice.

III. Securitatea şi integritatea reţelelor, a facilităţilor asociate şi a informaţiilor

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească o securitate fizică adecvată a reţelei şi a infrastructurii asociate (stabilirea şi menţinerea unor măsuri care să protejeze în mod corespunzător împotriva accesului fizic neautorizat, distrugerilor provocate de incendii, inundaţii, cutremure, explozii, tulburări publice şi alte forme de dezastre naturale sau provocate de oameni);

2) să stabilească o securitate adecvată a utilităţilor-suport, cum ar fi furnizarea de energie electrică, combustibil sau răcirea echipamentelor;

3) să stabilească măsuri de securitate adecvate pentru accesul (logic) la reţea şi la sistemele informatice;

4) să stabilească măsuri de securitate adecvate pentru a asigura protecţia reţelelor şi serviciilor de comunicaţii electronice împotriva codurilor cu potenţial dăunător, codurilor mobile neautorizate şi a atacurilor informatice, inclusiv DoS/DDoS.

IV. Managementul operaţiunilor

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească proceduri operaţionale şi responsabilităţi adecvate;

2) să stabilească proceduri privind managementul schimbărilor efectuate în reţeaua de comunicaţii electronice şi în software-urile de aplicaţii;

3) să stabilească proceduri de gestionare a resurselor astfel încât disponibilitatea şi starea acestora să fie verificată.

V. Managementul incidentelor

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească procese şi proceduri pentru managementul incidentelor care afectează securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice (care să vizeze raportarea internă, evaluarea, răspunsul la incidente şi escaladarea acestuia), inclusiv prin definirea rolurilor şi responsabilităţilor;

2) să stabilească un sistem de detectare a incidentelor;

3) să stabilească o procedură adecvată de raportare a incidentelor către Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii, precum şi către alte autorităţi responsabile, şi să stabilească planuri de comunicare a incidentelor către alte părţi externe (furnizori de reţele şi servicii de comunicaţii electronice afectaţi, media, clienţi, parteneri de afaceri etc.).

VI. Managementul continuităţii afacerii

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească o strategie pentru asigurarea continuităţii furnizării reţelelor şi serviciilor de comunicaţii electronice în situaţiile generate de perturbări grave ale funcţionării reţelei sau serviciului;

2) să deţină capabilităţi de implementare a strategiei de continuitate şi să stabilească planuri de continuitate şi de recuperare.

VII. Monitorizare, testare şi audit

Furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului au obligaţia:

1) să stabilească politici de monitorizare a sistemelor, precum şi politici privind jurnalele de sistem;

2) să stabilească politici pentru testarea, inclusiv prin exerciţii, a planurilor de continuitate şi de recuperare în cazul perturbărilor grave ale funcţionării reţelei sau serviciului;

3) să stabilească politici pentru testarea echipamentelor, sistemelor şi software-lor, în special înainte de conectarea/punerea lor în funcţiune;

4) să stabilească o politică adecvată pentru evaluarea şi testarea securităţii tuturor resurselor (echipamente, sisteme şi software etc.);

5) să stabilească o politică pentru monitorizarea conformităţii şi pentru audit, cu un proces de raportare a conformităţii şi de rezolvare a deficienţelor constatate în timpul auditului.