I. Virusul COVID-19 este un virus cu o răspândire extrem de largă la nivel mondial[1] iar Organizația Mondială a Sănătății (OMS) a afirmat că amenințarea unei pandemii a devenit foarte reală. Este îngrijorător faptul că atât de multe persoane/țări au fost afectate într-un timp atât de scurt. În momentul de față există cazuri de îmbolnăvire în toate țările din Europa, iar la nivel mondial s-a depășit numărul de 100 de țări afectate, conform OMS. Situația este îngrijorătoare mai ales în Italia unde s-a dispus chiar măsura închiderii granițelor.

În funcție de numărul total de îmbolnăviri, la nivel național au fost stabilite 4 stadii de alerte sanitare: 0-25 de cazuri stadiul I, 25-100 de cazuri stadiul II, 100-2000 de cazuri stadiul III, iar peste 2000 de cazuri stadiul IV. În Europa, alte țări cu niveluri ridicate de alertă sanitară sunt Franța, Spania sau Germania. Printre măsurile luate în vederea evitării răspândirii COVID-19 sunt: interzicerea organizării de evenimente de amploare, închiderea totală sau parțială a instituțiilor de învățământ[2] sau încurajarea telemuncii. Conform OMS, deciziile luate la nivel mondial de toți actorii implicați (guverne, întreprinderi, comunități, familii și indivizi) pot influența traiectoria acestei epidemii.

În contextul actual al răspândirii virusului COVID-19 au fost și vor fi și în continuare luate o serie de măsuri şi la nivelul țării noastre, măsuri ce vor implica o utilizare suplimentară a rețelelor şi serviciilor de comunicații electronice. Astfel, conform informațiilor existente până în prezent, în România sunt prevăzute deja unele măsuri în acest sens:

- La Ministerul Educației Naționale s-a constituit un grup care analizează posibilitatea efectuării cursurilor on-line. Pentru anul școlar 2019-2020, în învățământul preuniversitar, au fost înscriși aproximativ 2.8 milioane de elevi. Momentan nu s-a luat nici o decizie generalizată în ceea ce privește învățământul universitar. Conform datelor publice există un număr de aproximativ 400.000 de studenți pentru acest an universitar. În cazul unei decizii de închidere a acestor instituții de învățământ s-a discutat despre continuarea predării în mediul online.

- Guvernul României a anunțat în ședința de la Ministerul Afacerilor Interne din data de 9 martie, că se vor transmite circulare către toate instituțiile publice și persoanele juridice în vederea analizării posibilității desfășurării muncii la domiciliu, pentru o parte din personal, în temeiul dispozițiilor art. 108, 110 din Legea 53/2003 (Codul Muncii), respectiv potrivit Legii 81/2018 privind reglementarea activității de telemuncă, acolo unde este posibil. Astfel, se prevede o utilizare suplimentară a rețelelor și serviciilor de comunicații electronice la domiciliul angajaților. Mai mult decât atât, aceștia au nevoie de conexiuni stabile pentru a-și putea desfășura activitatea în condiții similare celor de la locul de muncă.

- O serie de organizații și instituții culturale au decis continuarea producțiilor şi transmiterea acestora în regim profesional, online, live, la orele programate în stagiune.

Toate aceste măsuri, coroborate cu numărul în creștere de persoane consemnate la domiciliu, în carantină sau autoizolare, sunt de natură să genereze un număr mare de conexiuni simultane de date/voce ce va conduce la un trafic suplimentar semnificativ, persistent, față de situațiile normale.

II. Conform dispozițiilor art. 3 din Decizia președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații nr. 512/2013 privind stabilirea măsurilor minime de securitate ce trebuie luate de către furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului și raportarea incidentelor cu impact

[1][1] http://www.cnscbt.ro/index.php/situatia-la-nivel-global-actualizata-zilnic

[2][2] https://en.unesco.org/themes/education-emergencies/coronavirus-school-closures

semnificativ asupra furnizării rețelelor și serviciilor de comunicații electronice, furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului (denumiți în continuare *furnizorii*) 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 şi rețelelor interconectate, având în vedere cele mai noi tehnologii și, acolo unde este cazul, de a colabora cu alți furnizori pentru implementarea acestor măsuri*. Totodată, furnizorii au obligația *de a lua toate măsurile de securitate necesare pentru a administra riscurile la adresa integrității rețelelor şi serviciilor de comunicații electronice, în scopul garantării integrității rețelelor şi al asigurării continuității furnizării serviciilor prin intermediul acestor rețele și, acolo unde este cazul, de a colabora cu alți furnizori pentru implementarea acestor măsuri*. Furnizorii au obligația *de a evalua şi, dacă este cazul, de a actualiza măsurile de securitate ori de câte ori este necesar, însă cel puțin o dată la 12 luni*.

Conform prevederilor deciziei menționate anterior, furnizorii au, printre altele[3], următoarele obligații:

1. 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, amenințărilor, vulnerabilităților, măsurilor existente şi a consecințelor pe care pierderea/încălcarea securității le-ar putea avea asupra resurselor;

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

d) să evalueze riscul;

e) să evalueze opțiunile 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;

2. să stabilească o structură adecvată a rolurilor şi responsabilităților în asigurarea securității și integrității rețelelor şi serviciilor;

3. să stabilească o politică cu privire la cerințele de securitate pentru achiziționarea de produse şi servicii de la terțe părți şi pentru asigurarea întreținerii sau gestiunii de către terțe părți a produselor şi serviciilor (servicii IT, software, interconectare, baze de date, facilități asociate etc);

4. să stabilească un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri și responsabilități;

5. să stabilească o strategie pentru asigurarea continuității furnizării rețelelor şi serviciilor de comunicații electronice în situațiile generate de perturbări grave ale funcționării rețelei sau serviciului;

6. să dețină capabilități de implementare a strategiei de continuitate şi să stabilească planuri de continuitate şi de recuperare;

---

[3][3] Toate domeniile vizate de măsurile de securitate se regăsesc în ANEXA nr. 1 a Deciziei președintelui ANCOM nr. 512/2013, disponibilă la adresa: https://www.ancom.ro/uploads/forms_files/decizie_2013_5121381320491.pdf

7. să stabilească politici pentru testarea, inclusiv prin exerciții, a planurilor de continuitate şi de recuperare în cazul perturbărilor grave ale funcționării rețelei sau serviciului.

III. Având în vedere contextul general prezentat mai sus, precum şi obligațiile legale care trebuie respectate cu privire la securitatea serviciilor şi rețelelor de comunicații electronice, în temeiul dispozițiilor art. 120 alin. (1) și (2) lit. a) din Ordonanța de urgență a Guvernului nr. 111/2011, vă solicităm să ne transmiteți, în mod complet și corect, următoarele informații:

1) Având în vedere obligația de la art. 3 alin. (4) din Decizia președintelui ANCOM nr. 512/2013 de a evalua şi dacă este cazul, de a actualiza măsurile de securitate ori de câte ori este necesar, însă cel puțin o dată la 12 luni, vă rugăm să ne transmiteți dacă ați efectuat un management al riscului, care să aibă în vedere amenințările introduse de contextul actual privind COVID-19?

2) Care sunt amenințările identificate precum şi riscurile la adresa asigurării securității rețelelor și serviciilor de comunicații electronice şi a continuității furnizării serviciilor?

3) Care sunt opțiunile de tratare a riscurilor identificate? Vă rugăm să precizați dacă ați stabilit mai multe niveluri de escaladare în funcție de concretizarea şi impactul amenințărilor identificate.

4) Pentru fiecare opțiune de tratare stabilită, vă rugăm să detaliați măsurile care au fost planificate/luate pentru minimizarea riscurilor identificate. De asemenea, vă rugăm să specificați în cazul fiecărei măsuri, care este domeniul[4] vizat.

5) A fost actualizată strategia privind asigurarea continuității furnizării rețelelor și serviciilor de comunicații electronice în contextul unei epidemii/pandemii? Au fost identificate şi asigurate capabilitățile/resursele necesare pentru implementarea strategiei privind asigurarea continuității furnizării rețelelor și serviciilor?

6) Există o structură adecvată a rolurilor şi responsabilităților în asigurarea securității rețelelor şi serviciilor precum şi un proces corespunzător de gestionare a schimbărilor de personal sau a modificărilor de roluri şi responsabilități în cazul unei epidemii/pandemii (indisponibilitatea unor angajați, dificultăți în intervenții care implică deplasarea echipelor de teren în vederea remedierii serviciilor etc.)? Detaliați.

7) Ați luat măsuri sau aveți plănuit să informați angajații în vederea reducerii expunerii și a transmiterii COVID-19? Dar abonații? Detaliați.

8) Ați luat sau aveți în vedere să luați măsuri pentru asigurarea continuității furnizării serviciilor în cazul creșterii traficului de date datorate izolării la domiciliu a populației (telemuncă, creșterea consumului de divertisment online, servicii suplimentare furnizate online etc.)? Care sunt acestea? Cu ce procent preconizați că va crește volumul de trafic în această situație?

9) Aveți planuri de continuitate în cazul în care subcontractorii nu vor putea furniza serviciile contractate (diminuare personal, întrerupere lanț de aprovizionare) şi impactează achiziționarea, operarea, întreținerea sau gestiunea echipamentelor, produselor sau serviciilor? Ați identificat posibile blocaje semnificative pe lanțul economic cauzate de întreruperea furnizării de echipamente/servicii? Ce măsuri ați luat/planificat?

10) Ați efectuat exerciții prin care să testați planurile de continuitate sau măsurile de securitate suplimentare identificate? În caz contrar, aveți în plan să efectuați astfel de exerciții?

[4] Domeniile vizate de măsurile minime de securitate din cadrul Anexei nr. 1 din Decizia președintelui ANCOM nr. 512/2013

11) Mențineți legătura cu instituțiile abilitate în managementul situațiilor de urgență? Aveți desemnată o persoană în acest scop?