I

(Резолюции, препоръки и становища)

РЕЗОЛЮЦИИ

СЪВЕТ

РЕЗОЛЮЦИЯ НА СЪВЕТА

от 18 декември 2009 година

относно европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност

(2009/C 321/01)

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

I. КАТО ВЗЕ ПРЕДВИД:

1. Съобщението на Комисията от 31 май 2006 г. относно „Стратегия за сигурност на информационното общество“, което предлага процес на „диалог, партньорство и оправомощаване“ с участието на държави-членки и заинтересовани страни от частния сектор;

2. Съобщението на Комисията от 12 декември 2006 г. относно „Европейска програма за защита на критичната инфраструктура“, която има за цел да повиши защитата на критичните инфраструктури в ЕС и да създаде рамка на ЕС за защита на критичните инфраструктури;

3. Директивата на Съвета от 8 декември 2008 г. относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита;

4. Резолюцията на Съвета от 22 март 2007 г. относно Стратегия за сигурност на информационното общество в Европа;

5. Заключенията на Съвета от 19—20 април 2007 г. относно европейска програма за защита на критичната инфраструктура;

6. Съобщението на Комисията от 30 март 2009 г. относно защитата на критичната информационна инфраструктура;

7. Продължаващото обсъждане, в т.ч. съответната обществена консултация, на бъдещето на Европейската агенция за мрежова и информационна сигурност (ENISA) и нейната роля при защитата на критичните информационни инфраструктури;

8. Заключенията на председателството относно защитата на критичните информационни инфраструктури след министерската конференция в Талин от 27—28 април 2009 г.;

9. Лисабонските цели за конкурентоспособност и растеж, както и извършваната понастоящем дейност за преглед на Лисабонската стратегия;

10. Мерките за сигурност, предложени при прегледа на регулаторната рамка за електронните съобщения, мрежи и услуги;

11. За да се гарантира ефективна бъдеща политика за мрежова и информационна сигурност, настоящата резолюция приема, че все още няма заключение за някакви необходими изменения в регламента относно ENISA. Тъй като понастоящем Комисията извършва преглед на бъдещето на политиката за мрежова и информационна сигурност, резултатите от този преглед по отношение всякакви изменения на регламента относно ENISA не следва да се предопределят от настоящата резолюция, преди Комисията да публикува резултатите си.

II. КАТО ОТБЕЛЯЗВА, ЧЕ:

1. Предвид значението на електронните съобщения, инфраструктури и услуги като основа за икономическата и социалната дейност, мрежовата и информационната сигурност допринася за важни обществени ценности и цели като демокрацията, неприкосновеността на личния живот, икономическия растеж, свободното изразяване на идеи, както и икономическата и политическата стабилност;

2. Системите, инфраструктурите и услугите на информационните и комуникационните технологии, в т.ч. интернет, играят жизненоважна роля за обществото и смущенията в тяхното функциониране притежават потенциал да причинят огромни икономически щети, което подчертава значението на мерките за по-голяма защита и устойчивост, насочени към гарантиране на непрекъснатост на критичните услуги;

3. Инцидентите, свързани със сигурността, има опасност да подкопаят доверието на потребителите. Докато сериозните смущения във функционирането на мрежовите и информационните системи могат да окажат значително икономическо и социално въздействие, ежедневните проблеми и неприятности също има опасност да навредят на общественото доверие в технологиите, мрежите и услугите;

4. Кръгът от заплахи се развива и разширява, което повишава необходимостта на крайните потребители, стопанските субекти и правителствата да се осигурят инфраструктури за електронни съобщения, които са стабилни и устойчиви по подразбиране, и да се установят правилните стимули за доставчиците, които своевременно да им ги предоставят;

5. Необходимо е мрежовата и информационната сигурност да се повиши и включи във всички области на политиката и всички обществени сектори, както и да се разгледа предизвикателството да се осигурят достатъчно умения посредством национални и европейски действия и повишаване на осведомеността сред потребителите на информационни и комуникационни технологии (ИКТ);

6. Завършването и функционирането на вътрешния пазар налага трансгранично сътрудничество между собствениците на мрежи и доставчиците на услуги, тъй като евентуални събития, водещи до смущения в една държава-членка, могат също да засегнат други държави-членки и ЕС като цяло;

7. Новите модели на потребление като концепциите „изчислителен облак“ (cloud computing) и „софтуер като услуга“ (SaaS) поставят допълнителен акцент върху значението на мрежовата и информационната сигурност;

8. Мрежовата и информационната сигурност обслужва целта на всички участници във всички обществени сектори да могат да имат доверие в информационните системи, поради което е необходим многосекторен и трансграничен подход;

9. С нарастващото използване на информационни и комуникационни технологии в обществото, мрежовата и информационната сигурност е предпоставка за надеждно, сигурно и безопасно предоставяне на обществени услуги, като тези на електронното управление.

10. ENISA има потенциал да разгърне важната си роля, която вече играе за мрежовата и информационната сигурност.

III. ПОДЧЕРТАВА, ЧЕ:

1. Високото равнище на мрежова и информационна сигурност в ЕС е необходимо, за да се подпомогнат:

   а) правата и свободите на гражданите, включително правото на неприкосновеност на личния живот;

   б) ефективното общество по отношение качеството на обработване на информацията;

   в) рентабилността и растежа на търговията и промишлеността;

   г) доверието на гражданите и организациите в обработката на информация и ИКТ системи;

2. Секторът на информационните и комуникационните технологии е от жизненоважно значение за повечето обществени сектори, което превръща осигуряването на мрежова и информационна сигурност в обща отговорност за всички заинтересовани страни, в т.ч. оператори, доставчици на услуги, доставчици на хардуер и софтуер, крайни потребители, публични органи и национални правителства.

IV. ОТЧИТА:

1. Значението на една активна европейска общност за мрежова и информационна сигурност с широки познания, която да допринася за засиленото сътрудничество между държавите-членки и частния сектор;

2. Предимствата от хармонизираното използване в ЕС на международните стандарти за сигурност за целите на мрежовата и информационната сигурност, когато е подходящо;

3. Необходимостта от европейски подход на сътрудничество по отношение на мрежовата и информационната сигурност в международен мащаб, тъй като това е предизвикателство със световно значение;

4. Значението, което има за държавите-членки и институциите на ЕС наличието на надеждни статистически данни за състоянието на мрежовата и информационната сигурност в Европа;

5. Необходимостта от повишаване на осведомеността и от средства за управление на риска за всички заинтересовани страни;

6. Значението на все по-големите усилия сред държавите-членки за повишаване на осведомеността, за обмен на добри практики и за разработване на насоки за държавите-членки;

7. Значението на модели с многостранно участие като публично-частните партньорства, изградени на основата на дългосрочен модел „отдолу нагоре“, за смекчаване на установените рискове, когато подобен подход придава добавена стойност на усилията за гарантиране на високо равнище на мрежова устойчивост;

8. Жизненоважната роля на доставчиците при осигуряването на стабилни и устойчиви инфраструктури за електронни съобщения на обществото;

9. Ползите от провеждането в Европа на учения в областта на мрежовата и информационната сигурност, които могат да предоставят ценни изводи за операторите на мрежи и доставчиците на услуги, както и за правителствата;

10. Че националните или правителствените екипи за действие при инциденти в информационната сигурност (CERT) или други механизми за действие, които реагират при заплахи и преодоляват уязвими аспекти, могат да допринесат за високо равнище на устойчивост и способност за устояване и възстановяване след смущения във функционирането на мрежовите и информационните системи;

11. Значението да се проучат стратегическите последствия, рискове и перспективи от създаването на CERT за институциите на ЕС и да се обмисли евентуална бъдеща роля на ENISA в тази област;

12. Извършената до момента дейност от ENISA в областта на мрежовата и информационната сигурност и необходимостта от допълнително развитие на ENISA в ефикасен орган с ясни ползи за европейската мрежова и информационна сигурност.

V. ИЗТЪКВА, ЧЕ:

1. За преодоляване на настоящите и бъдещите предизвикателства е от жизненоважно значение да се установи задълбочена и всеобхватна европейска стратегия за мрежова и информационна сигурност с ясно разграничени функции на Европейската комисия, държавите-членки и ENISA;

2. След подходяща консултация и анализ, в законодателния процес следва да се обмисли модернизирането и укрепването на ENISA с мандат, който гарантира гъвкавост и надзор от държавите-членки и Комисията, както и ефикасна роля на представителите на заинтересовани страни от частния сектор. Мандатът на агенцията следва да отчита регулаторната рамка за електронните съобщения, мрежи и услуги, да съответства на амбициозните стремежи, заложени в Лисабонската програма, и да включва цели, свързани с научните изследвания, иновациите, конкурентоспособността, икономическия растеж и осигуряването на доверие;

3. ENISA би могла да подпомага функциите на Комисията и държавите-членки за определяне и изпълнение на политиката, по-специално при преодоляване на несъответствията между технологии и политика, и следва да работи в тясно сътрудничество с държавите-членки и други заинтересовани страни, за да се гарантира, че дейностите ѝ са тясно съгласувани с приоритетите на ЕС;

4. Съгласно един преработен мандат ENISA следва да бъде център на ЕС за експертен опит по въпроси, свързани с мрежовата и информационната сигурност в ЕС. Европейските институции следва да търсят становището на агенцията като такъв център и да го отчитат в максимална степен при разработване и изпълнение на политики с потенциално въздействие в тази област;

5. ENISA би могла също при поискване да подпомага държавите-членки за усъвършенстване на техните собствени способности за мрежова и информационна сигурност и за преодоляване на инциденти, свързани със сигурността.

VI. ПРИКАНВА ДЪРЖАВИТЕ-ЧЛЕНКИ:

1. Да продължат дейността по засилване на доверието на крайните потребители в информационните и комуникационните технологии чрез кампании за повишаване на осведомеността;

2. Да организират национални учения и/или да участват в редовни европейски учения в областта на мрежовата и информационната сигурност, като се отбелязва необходимостта от задълбочено планиране поради сложността на материята и участието на частния сектор. При поискване ENISA би могла да оказва съдействие на държавите-членки в това отношение. Обхватът и географското измерение на ученията следва да се развиват по естествен път с времето и да се основават на признати рискове;

3. Да създадат екипи за действие при инциденти в информационната сигурност (CERT) в държавите-членки, които все още не са разработили такива способности, и да засилят сътрудничеството на европейско равнище между националните CERT. ENISA би могла да окаже съдействие на държавите-членки в това отношение;

4. Да увеличат усилията по програми за образование, обучение и научни изследвания в областта на мрежовата и информационната сигурност, за да гарантират наличието в ЕС на необходимите технически умения и професионалисти, както и да повишат професионализма на работещите в тази сфера;

5. Да действат съвместно при възникването на трансграничен инцидент и да повишат способностите си за предприемане на подходящи действия, което налага засилване на диалога между участниците, отговорни за вземането на решения, по-специално по свързаните с поверителността въпроси.

VII. ПРИКАНВА КОМИСИЯТА:

1. Да подпомага държавите-членки при изпълнението на настоящата резолюция, когато е целесъобразно;

2. Редовно да информира Европейския парламент и Съвета за предприети на равнище ЕС инициативи, свързани с мрежовата и информационната сигурност;

3. В сътрудничество с ENISA да започне кампания за повишаване на осведомеността сред европейските участници от публичния и частния сектор относно значението на подходящото управление на риска във връзка с мрежовата и информационната сигурност;

4. Съвместно с държавите-членки да продължи да установява стимули за доставчиците на инфраструктури за електронни съобщения, които да предоставят стабилни и устойчиви по подразбиране инфраструктури на крайните потребители, стопанските субекти и правителствата;

5. Съвместно с държавите-членки да разработи методи, които ще позволят да се извърши сравнителна оценка на равнище ЕС на социално-икономическото въздействие от инцидентите и на ефикасността на превантивните мерки;

6. Да насърчава и усъвършенства моделите с многостранно участие, които трябва да имат ясна добавена стойност в полза на крайните потребители и промишлеността;

7. Да представи всеобхватна стратегия за мрежова и информационна сигурност ([1]), включваща предложения за засилен и гъвкав мандат на ENISA, както и повишен надзор от държавите-членки и Комисията;

8. Съвместно с държавите-членки да извърши анализ на екипите за действие при инциденти в информационната сигурност (CERT), за да установи в кои области е необходимо допълнително сътрудничество;

9. Да продължи проучването на общ или оперативно съвместим подход за институциите на ЕС при обществени поръчки за сигурни ИКТ системи и услуги.

VIII. ПРИЗОВАВА ENISA:

1. Да продължи активно да подпомага държавите-членки, Европейската комисия и други заинтересовани страни при изпълнението на европейските политики за мрежова и информационна сигурност и плана за действие относно защитата на критичните информационни инфраструктури;

2. Да работи съвместно с държавите-членки, Комисията и статистическите органи по разработването на рамка от статистически данни за състоянието на мрежовата и информационната сигурност в Европа.

IX. ПРИКАНВА ЗАИНТЕРЕСОВАНИТЕ СТРАНИ:

1. Да активизират усилията за по-високо равнище на мрежова и информационна сигурност, по-специално по отношение предоставянето на продукти и услуги, които са надеждни, заслужаващи доверие и лесни за ползване;

2. Да информират точно потребителите за рисковете по отношение на сигурността, произтичащи от продуктите и услугите, и по какъв начин могат да се предпазят;

3. Да предприемат всички подходящи технически и организационни мерки за гарантиране на непрекъснатост, цялост и поверителност на електронните съобщителни мрежи и услуги;

4. Да продължат работата по стандартизация на мрежовата и информационната сигурност, като се стремят да открият хармонизирани и оперативно съвместими решения;

5. Да участват с държавите-членки в ученията, за да се предприемат подходящи действия при извънредни обстоятелства.

([1]) Комисията предлага тук да се добави думата „евентуално“.