ЕВРОПЕЙСКИ ПАРЛАМЕНТ 2009 - 2014

Комисия по промишленост, изследвания и енергетика

2010/0273(COD)

11.11.2011

СТАНОВИЩЕ

на комисията по промишленост, изследвания и енергетика

на вниманието на комисията по граждански свободи, правосъдие и вътрешни работи

относно предложението за директива на Европейския парламент и на Съвета относно атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Докладчик по становище: Christian Ehler

PA_Legam

ИЗМЕНЕНИЯ

Комисията по промишленост, изследвания и енергетика приканва водещата комисия по граждански свободи, правосъдие и вътрешни работи да включи в доклада си следните изменения:

Изменение 1

Предложение за директива
Съображение 1

Текст, предложен от Комисията	*Изменение*
(1) ***Основната цел*** на директивата е да сближи ***правилата относно*** наказателното право на държавите-членки в сферата на атаките срещу информационни системи и да подобри сътрудничеството между съдебните и другите компетентни органи, в това число полицията и други специализирани правоприлагащи служби на държавите-членки.	(1) ***Целта*** на директивата***, която*** е ***част от общата стратегия на Съюза за борба с организирана престъпност, укрепване на устойчивостта на компютърните мрежи, за защита на критичната информационна инфраструктура и за защитата на данните, е*** да сближи ***разпоредбите на*** наказателното право на държавите-членки в сферата на атаките срещу информационни системи и да подобри сътрудничеството между съдебните и другите компетентни органи, в това число полицията и други специализирани правоприлагащи служби на държавите-членки***, както и Комисията, Евроюст, Европол и Европейската агенция за мрежова и информационна сигурност, да даде възможност за общ и всеобхватен подход на Съюза***.

Изменение 2

Предложение за директива
Съображение 1 а (ново)

Текст, предложен от Комисията	*Изменение*
	(1а) Информационните системи представляват ключов елемент от политическото, социално и икономическо взаимодействие в

Европа. Все по-често и в по-голяма степен обществото зависи от подобни системи. Правилното функциониране и сигурността на тези системи в Европа е от жизненоважно значение за развитието на европейския вътрешен пазар, както и на конкурентоспособността и иновационната икономика. Като осигуряват огромни ползи информационните системи същевременно представляват и редица рискове за нашата сигурност поради тяхната сложност и уязвимост за различни видове компютърни престъпления. Следователно сигурността на информационните системи предизвиква постоянна загриженост, която изисква ефективен отговор от страна на държавите-членки и Съюза.

Изменение 3

Предложение за директива
Съображение 2

Текст, предложен от Комисията	*Изменение*
(2) Атаките срещу информационните системи, ***по-специално в резултат на заплахата от организираната престъпност***, представляват засилваща се опасност, а съществува и растяща загриженост от вероятни атаки по терористични или политически подбуди срещу ***информационните*** системи, които са част от критичната инфраструктура на държавите-членки и на Съюза. Това представлява заплаха за постигането на ***едно*** по-безопасно информационно общество и за изграждането на пространство на свобода, сигурност и правосъдие и следователно ***налага*** ответна реакция на	(2) Атаките срещу информационните системи ***могат да идват от различни извършители, като например терористи, организирани престъпни групи, държави или отделни лица. Те*** представляват засилваща се опасност ***за функционирането на информационните системи в Съюза и на глобално равнище***, а съществува и растяща загриженост от вероятни атаки по терористични или политически подбуди срещу ***информационни*** системи, които са част от критичната инфраструктура на държавите-членки и на Съюза. ***Равнището на посочената заплаха се увеличава значително***

равнището на Европейски съюз.	***поради трансграничния характер на определени престъпления и относително малкия риск и разходи за нарушителите, съчетани с огромни печалби, които могат да бъдат придобити и вредите, които могат да бъдат причинени чрез атаките.*** Това представлява заплаха за постигането на по-безопасно информационно общество и за изграждането на пространство на свобода, ***демокрация,*** сигурност и правосъдие***, подкопава създаването на европейски дигитален вътрешен пазар*** и следователно ***изисква*** ответна реакция на ***равнище*** Европейски съюз***, както и на международно равнище, например чрез Конвенцията на Съвета на Европа от 2001 г. за престъпления в кибернетичното пространство.***

Изменение 4

Предложение за директива
Съображение 2 а (ново)

Текст, предложен от Комисията	*Изменение*
	(2а) Неотдавнашни кибератаки, извършени срещу европейски мрежи или информационни системи причиниха съществени вреди на икономиката и сигурността на Съюза.

Обосновка

Имат се предвид кибератаките срещу европейските институции, извършени през март 2011 г., както и многобройните случаи на проникване в европейските схеми за търговия с емисии, които доведоха до кражби на емисии в размер на милиони евро.

Изменение 5

Предложение за директива
Съображение 3

Текст, предложен от Комисията	*Изменение*
(3) Има доказателства за наличието на тенденция към все по-опасни и постоянни широкомащабни атаки срещу информационните системи, които са от решаващо значение за държавите или за определени функции в публичния или частния сектор. Тази тенденция се придружава от разработка на все по-усъвършенствани инструменти, които могат да бъдат използвани от престъпници за започване на различни видове кибератаки.	(3) Има доказателства за наличието на тенденция към все по-опасни и постоянни широкомащабни атаки***, включително атаки за координирано блокиране на услуги,*** срещу информационните системи, които са от решаващо значение за ***международните организации,*** държавите***, за Съюза*** или за определени функции в публичния или частния сектор. ***Подобни атаки могат да предизвикат съществени икономически щети, както поради самото прекъсване на информационните системи и комуникации, така и поради загуба на важна от търговска гледна точка поверителна информация или други данни. Съществува опасност иновационни малки и средни предприятия, които зависят от правилното функциониране и достъпността на информационните системи, като същевременно могат да отделят по-малко ресурси за информационната сигурност, да бъдат особено засегнати.*** Тази тенденция се придружава от ***бърза*** разработка на ***информационни технологии и оттам на*** все по-усъвършенствани инструменти, които могат да бъдат използвани от престъпници за започване на различни видове кибератаки***, като част от тях имат значителен потенциал за причиняване на икономически и социални вреди***.

Изменение 6

Предложение за директива
Съображение 4

Текст, предложен от Комисията	*Изменение*
(4) Приемането на общи определения в тази област, по-конкретно за информационните системи и компютърните данни, е ***важно***, за да се осигури последователен подход в държавите-членки при прилагането на директивата.	(4) Приемането на общи определения в тази област, по-конкретно за информационните системи***, компютърните данни*** и ***престъпления по отношение на информационните системи и*** компютърните данни, е ***от съществено значение***, за да се осигури последователен ***и единен*** подход в държавите-членки при прилагането на директивата.

Изменение 7

Предложение за директива
Съображение 6

Текст, предложен от Комисията	*Изменение*
(6) Държавите-членки следва да предвидят наказания за атаките срещу информационните системи. Предвидените санкции следва да бъдат ефективни, пропорционални и възпиращи.	(6) ***В допълнение към мерките, предприети от*** държавите-членки***, Съюзът и частният сектор се стремят да повишат сигурността и целостта на информационните системи и да предотвратят атаки, както и да сведат до минимум въздействието от тях, държавите-членки*** следва да предвидят ***както ефективни мерки за предотвратяване на подобни атаки, така и хармонизирани*** наказания за атаките срещу информационните системи***, които следва да бъдат приети в рамките на по-широкомащабни национални стратегии за възпиране и борба с подобни атаки***. Предвидените санкции следва да бъдат ефективни, пропорционални и възпиращи. ***Постигането на сближаване при санкциите и наказанията, прилагани от държавите-членки, е необходимо поради често трансграничния характер на заплахите и е насочено***

	към намаляване на различията между държавите-членки, когато става въпрос за престъпления, извършени в рамките на Съюза.

Изменение 8

Предложение за директива
Съображение 6 а (ново)

Текст, предложен от Комисията	*Изменение*
	(6а) Държавите-членки, Съюзът и частният сектор, в сътрудничество с Европейската агенция за мрежова и информационна сигурност, следва да предприемат стъпки за увеличаване на сигурността и целостта на информационните системи, да предотвратяват атаки и да намаляват въздействието от атаките.

Изменение 9

Предложение за директива
Съображение 8

Текст, предложен от Комисията	*Изменение*
(8) В заключенията на Съвета от 27—28 ноември 2008 г. се посочва, че следва да се разработи нова стратегия с участието на държавите-членки и Комисията, като се вземе предвид съдържанието на Конвенцията на Съвета на Европа от 2001 г. за престъпленията в кибернетичното пространство. Конвенцията е референтната правна рамка за борба с престъпленията в кибернетичното пространство, включително и срещу атаките срещу информационните системи. Тази директива ***се основава*** Конвенцията.	(8) В заключенията на Съвета от 27—28 ноември 2008 г. се посочва, че следва да се разработи нова стратегия с участието на държавите-членки и Комисията, като се вземе предвид съдържанието на Конвенцията на Съвета на Европа от 2001 г. за престъпленията в кибернетичното пространство. ***Съветът и Комисията следва да насърчават държавите-членки, които още не са ратифицирали*** конвенцията***, да направят това възможно най-скоро. Конвенцията*** е референтната правна рамка за борба с престъпленията в кибернетичното пространство, включително и срещу

	атаките срещу информационните системи. Тази директива ***взема предвид съответните разпоредби на*** Конвенцията.

Изменение 10

Предложение за директива
Съображение 10

Текст, предложен от Комисията	*Изменение*
(10) Настоящата директива няма за цел да наложи наказателна отговорност за ***деяния извършени*** без престъпно намерение като, например, разрешените изпитвания или защитата на дадена компютърна система.	(10) Настоящата директива ***не обхваща действията, предприети с цел да гарантират сигурността на информационните системи, напр. способността на дадена информационна система да устои на престъпни деяния, във вида, в който са определени в настоящата директива, или да премахне инструменти, които са използвани или са предназначени за използване за подобни действия. Директивата също така*** няма за цел да наложи наказателна отговорност за ***случаи, при които обективните критерии, изброени в настоящата директива, са изпълнени, но деянието е извършено*** без престъпно намерение като, например, разрешените изпитвания или защитата на дадена компютърна система.

Обосновка

Като се има предвид, че границата между добросъвестен и недобросъвестен достъп понякога е неясна (автоматични актуализации и т.н.), изменението има за цел да изясни, че функционирането на софтуера за защита против вируси например или инструментите за отстраняване на вируси, или наблюдение на увредени устройства, са изцяло извън обхвата на директивата.

Изменение 11

Предложение за директива
Съображение 11

Текст, предложен от Комисията	*Изменение*
(11) С директивата се засилва значението на мрежите, като тази на Г—8 или Съвета на Европа, съставена от оперативни звена за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата с цел обмен на информация относно оказване на незабавно съдействие за разследвания и производства по престъпления, свързани с информационни системи или данни, или за събиране на доказателства в електронна форма за престъпления. Като се има предвид бързината, с която могат да бъдат извършени широкомащабни атаки, държавите-членки следва да реагират незабавно на спешни искания, отправени по тази мрежа от звена за контакт. Такова съдействие следва да включва улесняването или прякото вземане на мерки като, например: предоставяне на ***технически консултации***, опазване на данни, събирането на доказателства, предоставяне на правна информация и намирането на заподозрени лица.	(11) С директивата се засилва значението на мрежите, като тази на Г—8 или Съвета на Европа, съставена от оперативни звена за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата с цел обмен на информация относно оказване на незабавно съдействие за разследвания и производства по престъпления, свързани с информационни системи или данни, или за събиране на доказателства в електронна форма за престъпления ***или за намерение да се извърши престъпление***. Като се има предвид бързината, с която могат да бъдат извършени широкомащабни атаки, държавите-членки***, Съюзът и Европейската агенция за мрежова и информационна сигурност*** следва да реагират незабавно ***и ефективно*** на спешни искания, отправени по тази мрежа от звена за контакт. Такова съдействие следва да включва улесняването или прякото вземане на мерки като, например: предоставяне на ***техническа подкрепа***, ***включително по отношение на възстановяване на оперативността на информационната система,*** опазване на данни ***в съответствие с принципите за защита на личните данни***, събирането на доказателства, предоставяне на правна информация***, откриване на рискова и/или извлечена информация*** и намирането ***и установяването*** на ***самоличността на*** заподозрени лица.

Изменение 12

Предложение за директива
Съображение 11 а (ново)

Текст, предложен от Комисията	*Изменение*
	(11а) Сътрудничеството на публичните органи с частния сектор и гражданското общество е от голямо значение за превенцията и борбата с атаките срещу информационните системи. С посочените партньори следва да бъде установен постоянен диалог с оглед на широкото използване от тяхна страна на информационните системи и наложителното с оглед постигане на стабилно и правилно опериране на тези системи споделяне на отговорността. За създаването на култура в областта на сигурността на информационните технологии е важно да се повиши осведомеността на всички заинтересовани лица относно използването на информационните системи.

Изменение 13

Предложение за директива
Съображение 12

Текст, предложен от Комисията	*Изменение*
(12) Необходимо е да се събират данни за престъпления по настоящата директива, за да се добие по-цялостна представа за проблема на съюзно равнище и по този начин да се допринесе за изготвянето на по-ефективни отговори. Освен това данните ще помогнат на специализираните агенции като Европол и Европейската агенция за мрежова и информационна сигурност да оценят по-добре мащаба на престъпленията в кибернетичното пространство и състоянието на мрежовата и информационната сигурност в ***Европа***.	(12) Необходимо е да се събират данни за престъпления по настоящата директива, за да се добие по-цялостна представа за проблема на съюзно равнище и по този начин да се допринесе за изготвянето на по-ефективни отговори. ***Необходимо е държавите-членки, с подкрепата на Комисията и Европейската агенция за мрежова и информационна сигурност, да подобрят обмена на информация относно атаките срещу информационните системи.*** Освен това данните ще помогнат на специализираните ***органи и*** агенции като ***националните групи за бързо***

	реагиране по въпросите на информационната сигурност, Европол и Европейската агенция за мрежова и информационна сигурност да оценят по-добре мащаба на престъпленията в кибернетичното пространство и състоянието на мрежовата и информационната сигурност в ***Съюза, както и да подкрепят държавите-членки при приемането на ответна реакция срещу свързаните с информационната сигурност инциденти. По-доброто познаване на настоящи и бъдещи рискове ще помогне за вземането на по-подходящи решения относно възпирането, борбата или ограничаването на вредите, причинени от атаки срещу информационните системи.***

Изменение 14

Предложение за директива
Съображение 12 а (ново)

Текст, предложен от Комисията	*Изменение*
	***(12а) Докато настоящата директива следва да изпълни приложимите в наказателното право стриктни критерии за правна сигурност и предвидимост, необходимо е също така посредством разпоредбите на настоящата директива относно събирането на данни, обмена на информация и задължението на Комисията редовно да докладва за прилагането им и да представя всяко необходимо предложение, да се предвиди гъвкав механизъм, който да позволява адаптирането спрямо бъдещо развитие, което евентуално може да доведе до разширяване на обхвата на настоящата директива. Посоченото бъдещо развитие включва всяко технологично развитие, което**

позволява, например, по-ефективно прилагане в областта на атаките срещу информационните системи или улеснява предотвратяването или смекчаването на подобни атаки.

Обосновка

Въпреки че оценява въвеждането на наказания, един всеобхватен подход на Съюза за справяне с киберпрестъпността следва не само да се съсредоточи върху ефективното правоприлагане, но и да разработи стратегии и инструменти за предотвратяване на посочените престъпни деяния.

Изменение 15

Предложение за директива
Съображение 12 б (ново)

Текст, предложен от Комисията	*Изменение*
	(12б) Европейската агенция за мрежова и информационна сигурност следва да играе стратегическа роля в координирането на усилията на държавите-членки и на институциите на ЕС. На ENISA може, например, да бъде възложено да надзирава обмена на информация между тях, действайки по този начин като единно звено за контакт и регистър на инцидентите в областта на кибернетичната сигурност в Съюза. Може също така да й бъде възлагано да централизира статистически данни относно престъпленията, посочени в настоящата директива, на равнището на Съюза, както и да ги използват за основа при изготвянето на доклади относно състоянието на информационните системи и сигурността на компютърните данни в Съюза.

Изменение 16

Предложение за директива
Съображение 13

Текст, предложен от Комисията	*Изменение*
(13) Значителните пропуски и различия в законите на държавите-членки в тази област могат да препятстват борбата срещу организираната престъпност и тероризма, а също така да усложнят ефективното полицейско и съдебно сътрудничество в тази област. Транснационалният характер на съвременните информационни системи, които функционират отвъд националните граници, предполага, че атаките срещу тези системи често имат трансгранично измерение, което показва още веднъж спешната необходимост от осъществяване на действия за сближаване на ***наказателното*** право в тази област. Освен това координирането на наказателното преследване по дела за атаки срещу информационни системи ще стане по-лесно с приемането на Рамково решение 2009/948/ПВР на Съвета относно предотвратяване и уреждане на спорове за упражняване на компетентност при наказателни производства.	(13) Значителните пропуски и различия в законите на държавите-членки в тази област могат да препятстват борбата срещу организираната престъпност и тероризма, а също така да усложнят ефективното полицейско и съдебно сътрудничество в тази област. Транснационалният характер на съвременните информационни системи, които функционират отвъд националните граници, предполага, че атаките срещу тези системи често имат трансгранично измерение, което показва още веднъж спешната необходимост от осъществяване на действия ***на равнище на Съюза*** за сближаване на ***националното наказателно*** право в тази област. ***Също така Съюзът следва да работи за постигането на по-тясно международно сътрудничество в областта на сигурността на мрежовите и информационни системи, което да включва всички заинтересовани международни субекти.*** Освен това координирането на наказателното преследване по дела за атаки срещу информационни системи ще стане по-лесно с приемането на Рамково решение 2009/948/ПВР на Съвета относно предотвратяване и уреждане на спорове за упражняване на компетентност при наказателни производства.

Изменение 17

Предложение за директива
Член 1 – параграф 1

Текст, предложен от Комисията	*Изменение*
С директивата се определят	С директивата се определят

престъпленията в областта на атаките срещу информационните системи и се установяват минимални правила за налагане на наказания за такива престъпления. С нея се цели също създаването на общи разпоредби за предотвратяване на подобни атаки и подобряване на европейското сътрудничество в ***областта на наказателното правосъдие***.	престъпленията в областта на атаките срещу информационните системи и се установяват ***хармонизирани*** минимални правила за налагане на наказания за такива престъпления. С нея се цели също създаването на общи разпоредби ***както*** за предотвратяване, ***така и за борба с*** подобни атаки и ***за*** подобряване на европейското сътрудничество в ***тази област, особено по отношение на наказателното правосъдие***.

Изменение 18

Предложение за директива
Член 2 – буква г)

Текст, предложен от Комисията	*Изменение*
г) „неправомерен“ означава достъп или намеса, който/която не е разрешен/а от собственика или от други притежатели на права върху системата или части от нея, или е забранен/а по силата на националното законодателство.	г) „неправомерен“ означава достъп или намеса, който/която не е разрешен/а от собственика или от други притежатели на права върху системата или части от нея, или е забранен/а по силата на националното ***или европейското*** законодателство.

Изменение 19

Предложение за директива
Член 7 – буква б)

Текст, предложен от Комисията	*Изменение*
б) компютърна парола, код за достъп или други подобни данни, с чиято помощ може да се получи достъп до информационна система или до част от нея,	б) компютърна парола, код за достъп, ***цифров или материален символ,*** или други подобни данни, с чиято помощ може да се получи достъп до информационна система или до част от нея.

Изменение 20

Предложение за директива
Член 8 – параграф 1 а (нов)

Текст, предложен от Комисията	*Изменение*
	1а. Държавите-членки гарантират, че непозволеното предаване на идентификационни данни на други лица с цел осъществяване на някоя от дейностите, посочени в членове 3–7, съставлява престъпление.

Изменение 21

Предложение за директива
Член 8 – параграф 1 б (нов)

Текст, предложен от Комисията	*Изменение*
	1б. Държавите-членки гарантират, че престъпление по смисъла на членове 3–7, извършено от лице, което в рамките на своята заетост разполага с достъп до системите за сигурност на информационни системи, се третира като утежняващо вината обстоятелството и съставлява престъпление.

Изменение 22

Предложение за директива
Член 10 – параграф 2

Текст, предложен от Комисията	*Изменение*
2. Държавите-членки вземат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 3—6, се наказват с лишаване от свобода за максимален срок не по-малък от пет години, когато те са извършени чрез използване на инструменти, предназначени за започване на атаки, засягащи значителен брой информационни системи, или на атаки, причиняващи значителни щети като,	2. Държавите-членки вземат необходимите мерки, за да гарантират, че престъпленията, посочени в членове 3—6, се наказват с лишаване от свобода за максимален срок не по-малък от пет години, когато те са извършени чрез използване на инструменти, предназначени за започване на атаки, засягащи значителен брой информационни системи, или на атаки, причиняващи значителни щети като,

например, прекъснати системни услуги, финансови разходи или загуба на лични данни.	например, прекъснати системни услуги, финансови разходи или загуба на лични данни***, или чувствителна информация***.

Изменение 23

Предложение за директива
Член 13 – параграф 1 – буква в

Текст, предложен от Комисията	*Изменение*
в) в полза на юридическо лице, ***чието главно управление е разположено*** на територията на съответната държавата-членка.	в) в полза на юридическо лице, ***установено*** на територията на тази държава-членка.

Изменение 24

Предложение за директива
Член 14 – параграф 1

Текст, предложен от Комисията	*Изменение*
1. За целите на обмена на информация, свързана с престъпленията, посочени в членове 3—8, и в изпълнение на изискванията относно защитата на данни, държавите-членки използват ***съществуващата мрежа*** от оперативни звена за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата. Държавите-членки гарантират също, че разполагат с процедури, чрез които да отговарят на спешни искания в максимален срок от осем часа. ***В този отговор се посочва поне дали, кога и под каква форма ще бъде отговорено на искането за помощ.***	1. За целите на обмена на информация, свързана с престъпленията, посочени в членове 3—8, и в изпълнение на изискванията относно защитата на данни, държавите-членки ***гарантират, че разполагат с оперативно национално звено за контакт и*** използват ***мрежата*** от оперативни звена за контакт, които са на разположение 24 часа в денонощието и седем дни в седмицата***, както и че предават съответната информация на Комисията и на Европейската агенция за мрежова и информационна сигурност***. Държавите-членки гарантират също, че разполагат с процедури, чрез които да отговарят на спешни искания в максимален срок от осем часа. Този отговор ***е ефективен и включва, при необходимост, улесняването или на прякото прилагане на следните мерки:***

	предоставяне на техническа консултация, включително по отношение на възстановяване на оперативността на информационната система, опазване на данни в съответствие с принципите за защита на личните данни, събирането на доказателства, предоставяне на правна информация и намирането и установяването на самоличността на заподозрени лица. Звената за контакт посочват формата и сроковете, в които следва да се предостави отговор на исканията за помощ.

Изменение 25

Предложение за директива
Член 14 – параграф 2

Текст, предложен от Комисията	*Изменение*
2. Държавите-членки информират Комисията за определеното от тях звено за контакт относно обмена на информация за престъпления, посочени в членове 3—8. Комисията съобщава тази информация на другите държави-членки.	2. Държавите-членки информират Комисията***, Евроюст и Европейската агенция за мрежова и информационна сигурност*** за определеното от тях звено за контакт относно обмена на информация за престъпления, посочени в членове 3—8. Комисията съобщава тази информация на другите държави-членки.

Изменение 26

Предложение за директива
Член 15 – параграф 3

Текст, предложен от Комисията	*Изменение*
3. Държавите-членки предават на Комисията събраните по този член данни. ***Те*** правят също необходимото ***консолидираният*** преглед на тези статистически отчети да бъде	3. Държавите-членки предават на Комисията***, Европол и Европейската агенция за мрежова и информационна сигурност*** събраните по този член данни ***и*** правят също така необходимото

публикуван.	***периодичен консолидиран*** преглед на тези статистически отчети да бъде публикуван.

Изменение 27

Предложение за директива
Член 18 – параграф 1

Текст, предложен от Комисията	*Изменение*
1. До [ЧЕТИРИ ГОДИНИ СЛЕД ПРИЕМАНЕТО] и на всеки три години след това Комисията представя на Европейския парламент и на Съвета доклад за прилагането на директивата в държавите-членки, който съдържа и всяко необходимо предложение.	1. До [ЧЕТИРИ ГОДИНИ СЛЕД ПРИЕМАНЕТО] и на всеки три години след това Комисията, ***след консултация с всички заинтересовани субекти,*** представя на Европейския парламент и на Съвета доклад за прилагането на директивата в държавите-членки, който съдържа и всяко необходимо предложение. ***Всеки доклад посочва и взема предвид всяко необходимо предложение, технически решения, които позволяват по-ефективно прилагане в Съюза в областта на атаките срещу информационните системи, включително технически решения, които могат да послужат за предотвратяване или смекчаване на подобни атаки.***

Изменение 28

Предложение за директива
Член 18 – параграф 2

Текст, предложен от Комисията	*Изменение*
2. Държавите-членки изпращат на Комисията цялата информация, необходима за изготвянето на посочения в параграф 1 доклад. Информацията съдържа подробно описание на законодателните и незаконодателните мерки в приложение на настоящата директива.	2. Държавите-членки ***и Европейската агенция за мрежова и информационна сигурност*** изпращат на Комисията цялата информация, необходима за изготвянето на посочения в параграф 1 доклад. Информацията съдържа подробно описание на законодателните и незаконодателните мерки в приложение на настоящата директива.

ПРОЦЕДУРА

Заглавие	Атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета
Позовавания	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)
Водеща комисия Дата на обявяване в заседание	LIBE 7.10.2010 г.
Подпомагаща(и) комисия(и) Дата на обявяване в заседание	ITRE 7.10.2010 г.
Докладчик(ци) Дата на назначаване	Christian Ehler 24.11.2010 г.
Разглеждане в комисия	13.4.2011 г. 6.10.2011 г.
Дата на приемане	10.11.2011 г.
Резултат от окончателното гласуване	+: 49 –: 0 0: 1
Членове, присъствали на окончателното гласуване	Ivo Belet, Bendt Bendtsen, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Ioan Enciu, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Jacky Hénin, Kent Johansson, Romana Jordan Cizelj, Lena Kolarska-Bobińska, Béla Kovács, Philippe Lamberts, Bogdan Kazimierz Marcinkiewicz, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Aldo Patriciello, Anni Podimata, Miloslav Ransdorf, Herbert Reul, Michèle Rivasi, Jens Rohde, Paul Rübig, Amalia Sartori, Francisco Sosa Wagner, Konrad Szymański, Michael Theurer, Ioannis A. Tsoukalas, Claude Turmes, Niki Tzavela, Marita Ulvskog, Владимир Уручев, Adina-Ioana Vălean
Заместник(ци), присъствал(и) на окончателното гласуване	Antonio Cancian, Jolanta Emilia Hibner, Yannick Jadot, Ивайло Калфин, Bernd Lange, Werner Langen, Markus Pieper, Mario Pirillo, Hannes Swoboda, Silvia-Adriana Ţicău
Заместник(ци) (чл. 187, пар. 2), присъствал(и) на окончателното гласуване	Eider Gardiazábal Rubial