ALLIANCE OF LIBERALS AND DEMOCRATS FOR EUROPE

Киберсигурност

Киберсигурност

Това издание се реализира по инициатива на
Искра Михайлова, с
финансовата подкрепа на групата на АЛДЕ.
София,
2018

Съдържание

Въведение

Киберсигурността е от критично значение както за нашето благополучие, така и за сигурността ни. Нашето ежедневие и икономиките ни стават все по-зависими от цифровите технологии, а с това ние ставаме все по-уязвими. Инцидентите, свързани с киберсигурността, стават все по-разнообразни по отношение на това кой ги извършва и какво се стреми да постигне. Злонамерените дейности в киберпространството застрашават не само нашите икономики и усилията за цифров единен пазар, но и самото функциониране на нашите демокрации, свободи и ценности. Бъдещата ни сигурност зависи от реформирането на способността ни да защитим ЕС от киберзаплахи: както гражданската инфраструктура, така и военният капацитет разчитат на надеждни цифрови системи. Това бе признато от Европейския съвет през юни 2017 г. и в Глобалната стратегия за външната политика и политика на сигурност на Европейския съюз.

Всеки ден в интернет циркулират около 150 000 компютърни вируса и 148 000 компютъра биват компрометирани. Според Световния икономически форум има 10-процентна вероятност от значителен срив на критична информационна инфраструктура през следващото десетилетие, което би могло да нанесе щети от 250 млрд. щатски долара.

Киберпрестъпността причинява немалък дял от инцидентите в киберпространство, Symantec[1] счита, че жертвите на киберпрестъпленията в световен мащаб губят около 290 млрд. евро всяка година, докато според проучване на McAfee[2] приходите за киберпрестъпността са 750 млрд. евро годишно.

Според обществената консултация относно мрежовата и информационна сигурност (МИС) през последните години 56,8 % от анкетираните са преживели инциденти, свързани с МИС, с тежко въздействие върху дейността им. Рисковете нарастват експоненциално. Проучванията показват, че между 2013 г. и 2017 г. икономическото въздействие на киберпрестъпността е нараснало петкратно, а до 2019 г. може да се увеличи още четири пъти . Особено голям ръст се наблюдава при софтуера за изнудване, като последните атаки отразяват рязкото нарастване на престъпната дейност в киберпространството. Обаче софтуерът за изнудване далеч не е единствената съществена заплаха.

1 Symantec е софтуерна компания, водеща в доставянето на решения за сигурността
2 McAfee е водеща американска компания в областта на киберсигурността.

Инцидентите в областта на киберсигурността стават все по-чести, по-значителни и по-комплексни и за тях няма граници. Тези инциденти могат да причинят значителни щети на безопасността и на икономиката. Усилията за предотвратяване, сътрудничество и по-голяма прозрачност по отношение на инцидентите в киберпространство трябва да се засилят. Досегашните усилия на Европейската комисия и отделни държави членки бяха твърде разпокъсани, за да се справят с нарастващото предизвикателство.

Киберзаплахите произхождат както от недържавни, така и от държавни участници: често са криминални и имат за цел печалба, но могат да бъдат и политически и стратегически. Опасността от престъпления се засилва поради размиването на границата между киберпрестъпността и обичайната престъпност, тъй като престъпниците използват интернет едновременно за увеличаване на мащаба на действията си и като източник за намиране на нови методи и средства за извършване на престъпление. Въпреки това в повечето случаи шансовете за издирване на престъпника са минимални, а за съдебното му преследване — още по-малки. Същевременно държавните участници все по-често постигат своите геополитически цели не само с традиционни средства като военна сила, а също и чрез по-дискретни киберинструменти, включително намеса във вътрешните демократични процеси. Сега широко се признава, че киберпространството се използва като бойно поле — самостоятелно или като част от хибриден подход. Все по-често се срещат кампании за дезинформация, фалшиви новини и кибероперации, насочени към критичната инфраструктура, и те изискват съответен отговор.

Ако не подобрим съществено нашата киберсигурност, рискът ще нараства успоредно с цифровизацията. До 2020 г. се очаква към интернет да бъдат свързани десетки милиарди устройства от „интернет на нещата“[3], но киберсигурността все още не е приоритет при тяхното проектиране. Ако не успеем да защитим устройствата, които ще управляват нашите електропреносни мрежи, автомобили и транспортни мрежи, заводи, финанси, болници и домове, това може да има разрушителни последици и силно да разклати доверието на потребителите в нововъзникващите технологии. Рискът от политически мотивирани атаки към граждански цели и от слабости във военната киберотбрана още повече засилва тази опасност.

Необходимо е да се създаде по-голяма устойчивост и стратегическа автономност, като се увеличат възможностите по отношение на технологии и умения и се подпомогне изграждането на силен единен пазар. Това изисква да се създадат подходящите структури за изграждане на силна киберсигурност и за реагиране при

3 „Интернет на нещата“е концепция за компютърна мрежа от физически обекти (устройства, превозни средства, сгради и други предмети и вещи), притежаващи вградени електронни устройства за взаимодействие помежду си или с външната среда. Тази концепция разглежда организацията на такива мрежи като явление, способно да преустрои икономическите и обществени процеси така, че да изключи необходимостта от участие на човека в част от действията и операциите.

нужда, с участие в най-висока степен на всички ключови действащи лица. Освен това е наложително да се работи в посока на подобрено възпиращо действие за кибератаките чрез по-успешна работа за откриване, проследяване и търсене на отговорност на съответните лица.

ЕС вече работи по много от тези въпроси: сега е време да се обединят различните работни направления. През 2013 г. ЕС прие Стратегия за киберсигурност, поставяйки началото на ключови работни направления за повишаване на устойчивостта на киберпространството. Главните цели и принципи на тази стратегия за насърчаване на надеждна, безопасна и отворена кибернетична екосистема остават валидни.

Постоянно развиващият се и задълбочаващ се контекст на киберзаплахите обаче изисква допълнителни действия за устояване на атаките и предотвратяване на такива атаки в бъдеще.

ЕС е добре подготвен за обезпечаване на киберсигурността предвид обхвата на неговите политики и инструментите, структурите и способностите, с които разполага. Макар държавите членки да продължават да носят отговорността за националната сигурност, мащабът и трансграничният характер на заплахата показват необходимостта от действия на Съюза, които да насърчават и подпомагат държавите членки да развиват и поддържат повече и по-добри национални възможности за киберсигурност, като същевременно се изгражда такъв капацитет на равнище ЕС. Този подход има за цел да стимулира всички участници — ЕС, държавите членки, предприятията от сектора и отделните лица — да издигнат киберсигурността в приоритет, което е нужно, за да се изгради устойчивост и да се осигури по-добра реакция на ЕС на кибератаки.

В свое Съвместно съобщение до Европейския парламент и Съвета относно Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС от 13.9.2017 г., Европейската комисия предлага подход, който да осигури конкретни стъпки, за да се подпомогне откриването и разследването на всички видове киберинциденти, насочени срещу ЕС и срещу неговите държави членки, и за да се реагира по подходящ начин, включително чрез съдебно преследване на престъпниците. Той ще даде възможност външната дейност на ЕС ефективно да повиши киберсигурността в световен мащаб. В резултат на това ЕС ще промени подхода си от реактивен на проактивен, за да защити европейското благополучие, общество и европейските ценности, както и основните права и свободи, като реагира както на съществуващите, така и на бъдещи заплахи.

Киберсигурност

ГЛАВНИТЕ КИБЕР ЗАПЛАХИ

Малуер
(на английски: malware)

зловреден софтуер, който е специално създаден, за да се снабди с достъп и/или да навреди на компютъра без знанието на собственика.

Компютърните червеи
(на английски: worms)

програми, подобни на вирусите, но нямат нужда от определен носител или човешка намеса, за да се разпространят. Обикновено използват електронна поща или друг транспортен механизъм, за да се копират.

Компютърен вирус
(на английски: virus)

опасен софтуер, който се разпространява от един компютър на друг като оставя инфектирани компютрите, през които преминава. Вирусите варират от почти безобидни до такива, които повреждат или крадат информация, забавят и дори спират работата на компютърната система, извеждат на екрана нежелано съдържание или да причинят некоректно изпълнение на някоя програма.

Троянци
(на английски: trojans)

тези софтуери проникват в компютърните системи като наподобяват легитимни програми, които потребителят би искал да стартира. След като се активират, те могат да причинят множество щети на системата. Троянците са известни и това, че могат да създадат така наречените „задни врати“ , които дават възможност за нелегитимен достъп до системата.

Фишинг
(на английски: phising)

злонамерен опит за придобиване на чужди данни. Целта е да се придобият потребителски имена, пароли и финансови данни. Извършителят на атаката използва фалшиви имейли и сайтове, за да привлече потребителите.

Спайуер
(на английски: spyware)

софтуер, който след инсталацията си започва да събира информация за системата и я изпраща, където е програмиран да я изпраща.

Стратегията за киберсигурност

„ОТВОРЕНО, БЕЗОПАСНО И СИГУРНО КИБЕРПРОСТРАНСТВО"

Стратегията за киберсигурност „Отворено, безопасно и сигурно киберпространство" представлява цялостната визия на ЕС за това как най-добре да се предотвратяват кибернетични смущения и атаки и да се отговаря на тях. Целта е насърчаване на европейските ценности свобода и демокрация и осигуряване на безопасния растеж на цифровата икономика. Конкретните дейности са насочени към засилване на устойчивостта на информационните системи в киберпространство, намаляване на киберпрестъпността и укрепване на международната политика за киберсигурността и киберотбраната на ЕС.

В стратегията се представя визията на ЕС за кибернетична сигурност по отношение на *пет приоритета*:

- Постигане на *устойчивост* в киберпространство;
- Чувствително *намаляване* на киберпрестъпността;
- Разработване на *политика за киберотбрана* и способности, свързани с общата политика за сигурност и отбрана (ОПСО);
- Разработване на промишлени и технологични *ресурси* за киберсигурност;
- Създаване на съгласувана *международна политика* на Европейския съюз за киберпространството и насърчаване на основните ценности на ЕС.

Международната политика на ЕС за киберпространството насърчава зачитането на основните ценности на ЕС, определя стандарти за отговорно поведение, защитава прилагането на съществуващите международни закони в киберпространството, като подпомага държави извън ЕС при изграждането на капацитет за киберсигурността и насърчава международното сътрудничество по проблеми в киберпространство.

В Стратегията за киберсигурност на Европейския съюз се прави оценка, че през последните две десетилетия Интернет като цяло и в по-широк аспект киберпространството оказват изключително влияние върху обществата и тяхното развитие в различни области: ежедневен живот, социално взаимодействие, фундаментални права, икономика, сигурност и т.н. Благодарение на своите особености, киберпространството премахва бариерите на физическите и географските граници между отделните страни и техните граждани, като в същото време създава условия за споделяне на данни и информация в глобален мащаб.

Информационните и комуникационните технологии се превръщат в гръбнака на икономическото развитие и в същото време представляват критично важен ресурс за икономическия сектор. Успоредно с нарастването на свободата на потребителите в киберпространството, нараства и потребността от защита на техните права и като цяло защита на принципите на демократичното общество и валидността на закона. В документа се прави констатацията, че свободата на on-line услугите и комуникациите се нуждае без съмнение от защитеност и сигурност. Водещата роля в това направление се делегира на отделните държави. От друга страна, частният бизнес се определя като един от големите собственици и потребители в киберпространството, което определя значимостта на неговото място и неговата роля и отговорности за създаване на сигурно киберпространство.

Особено внимание в съдържанието на стратегията на ЕС за киберсигурност се обръща на оценката за това, че случващото се през последните години от една страна доказва предимствата и възможностите, които киберпространството предлага, но от друга страна категорично подчертава уязвимостите пред сигурността на това пространство. Броят на инцидентите с киберсигурността, които в огромната си част са с международен характер, нараства с алармиращи темпове и води до създаване на различен тип кризи в различни области на социално-икономическия живот: кризи със сигурността на веригите за доставка на стоки и услуги; кризи с управлението и функционирането на обекти от критичната инфраструктура и т.н. Оценката на заплахите за киберсигурността по отношение на техния източник е категорична и включва организираната престъпност, международния тероризъм, политически мотиви, държавно спонсорирани атаки, природни бедствия, неумишлени и умишлени човешки действия и др. Характерна особеност е стремежът на киберпрестъпниците да развиват и използват все по-нови, усъвършенствани и иновативни методи и инструменти за добиване на нерегламентиран достъп до компютърни системи и мрежи, кражба на чувствителна информация, извършване на икономически шпионаж и т.н. В страните извън ЕС съществуват държави, чиито правителства използват киберпространството за наблюдение и контролиране на дейността и живота на гражданите.

В стратегията на ЕС са посочени основните принципи, които служат като основа или като фундамент при създаване на политики, разработване и прилагане на мерки за постигане на приемливо ниво на киберсигурност на регионално равнище. Тези принципи се отнасят до следното:

» прилагане на политики, процедури и мерки за киберсигурност, които отговарят и защитават ключовите ценности на Европейския съюз;

» защита на фундаменталните права на всички актьори в киберпространството, защита на свободата на словото, личното пространство, личните данни и

идентичността на гражданите;

» осигуряване на достъп на всеки потребител до Интернет, предлаганите услуги и публичните потоци от информация;

» изграждане и прилагане на ефективни модели за управление в киберпространството, зачитащи демократичните ценности при участие на всички заинтересовани страни;

» споделена отговорност на всички участници в киберпространството по отношение на гарантиране на сигурността.

ЕС е решен да опази онлайн средата, осигурявайки възможно най-голяма свобода и сигурност, в полза на всички. Тази стратегия се приема съвместно от Комисията и от Върховения представител на Европейския съюз по въпросите на външните работи и политиката на сигурност. Тя очертава визията на ЕС в тази област, изяснява ролите и отговорностите и предлага специфични дейности на ниво ЕС. Нейната цел е да осигури силна и ефективна защита и насърчаване на правата на гражданите, за да направи онлайн средата на ЕС най-сигурната в света.

Във фокуса на дейностите и мерките за постигане на киберсигурност на *регионално равнище* са поставени няколко основни зависимости. На първо място в стратегията на ЕС за киберсигурност се посочва стремежа към балансиране на достъпността до киберпространството и сигурността на същото това пространство. Очевидна е обратно пропорционалната зависимост, която свързва тези два параметъра: при увеличаване на достъпността ще намалее сигурността на услугите в киберпространството и обратно – засилването на мерките за сигурност като следствие ще снижат достъпността до предлаганите услуги. Търсенето на *баланс между достъпност и сигурност* се затруднява от една страна предвид динамичния характер на промените в киберпространството и от друга страна за сметка на необходимостта от постигане на баланс на различни нива и между желанията на различни участници в киберпространството. Друга зависимост определя отделните държави като носители на основната отговорност за справяне с предизвикателствата пред киберсигурността. В своята цялост, дейностите и мерките, които ЕС определя в стратегията за киберсигурност, могат да бъдат определени като краткосрочни и дългосрочни, включващи изискванията на разнообразни политически документи, изпълнявани от различен тип участници, опериращи в киберпространството. Всички предвидени мерки и дейности на регионално равнище обслужват зададените в стратегията приоритети, които могат да бъдат определени по следния начин:

» постигане на киберсигурност, която в последствие да прерасне в кибер

устойчивост: ключов момент при изграждане на среда за киберсигурност на регионално ниво и възможности за противодействие срещу киберпрестъпността е създаване на общи способности и процедури за ефективно взаимодействие;

» Съществен компонент на процеса по изграждане на пакет от способности за киберсигурност е обучението на всички участници в киберпространството за разпознаване и противодействие срещу инциденти от различен тип;

» нарастване на степента на готовност за отговор на инциденти с киберсигурността: в основата на този приоритет стои разбирането за това, че киберсигурността представлява обща и споделена отговорност на страните от ЕС, на държавните институции, частния бизнес, академичната общност и отделните потребители. Нещо повече, в стратегията за киберсигурност на ЕС се прави оценката, че крайните потребители на услугите в киберпространството играят ключова роля при осигуряване на сигурността на компютърните системи и мрежи;

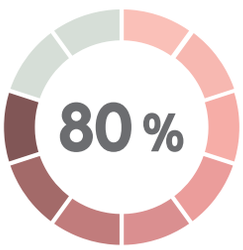
» снижаване на размерите на киберпрестъпността в нейните различни нюанси (области): в анализираната стратегия се подчертава факта, че киберпрестъпността към момента е най-бързо развиващата се престъпност на регионално равнище (като пример: за един ден броят на жертвите на киберпрестъпления в световен мащаб се оценява на един милион души). Мерките за повишаване на ефективността на противодействието срещу киберпрестъпността следва да отчитат особеностите на киберпрестъпленията, каквито са: използването на нови технологии; сравнително нисък риск за престъпниците; наличие на висока мотивация, идваща от възможностите за извличане на значителни ползи, в това число и финансови и т.н.

» изграждане на оперативни способности за противодействие срещу киберпрестъпленията: в този аспект в стратегията за киберсигурност на ЕС се прави оценка, че правоприлагащите органи не са в състояние да противодействат по един достатъчно ефективен начин на киберпрестъпленията с помощта на традиционните методи и средства или поне не без комбиниране на традиционните методи и средства със специфични инструменти, отговарящи на особеностите на този вид престъпност. В стратегията се препоръчва на страните да обърнат внимание върху изграждането на специализирани структури и способности за противодействие срещу киберпрестъпността, които освен всичко друго да предполагат достатъчно ефективно международно сътрудничество;

» подобряване на координацията на ниво ЕС при изграждане на среда за киберсигурност и противодействие срещу киберпрестъпленията.

Споразумение в областта на киберсигурността с отрасъла

На 05 юли 2016 г. Комисията стартира ново публично-частно партньорство в областта на киберсигурността, от което се очаква до 2020 г. да доведе до инвестиции в размер на 1,8 милиарда евро. Това е част от поредица от инициативи с цел подобряване на устойчивостта на Европа срещу кибератаки и засилване на конкурентоспособността на сектора на киберсигурността.



Според неотдавнашно проучване, най-малко 80 % от европейските дружества през последната година са имали поне един инцидент, свързан с киберсигурността. Това нанася вреда на европейските дружества, независимо дали са големи или малки, и застрашава доверието в цифровата икономика. Като част от своята Стратегия за цифров единен пазар Комисията иска да засили трансграничното сътрудничество в трансграничен аспект и между всички участници и сектори, активни в областта на киберсигурността, както и да подпомогне разработването на новаторски и сигурни технологии, продукти и услуги в целия ЕС.

Планът за действие включва стартирането на първото европейско публично-частно партньорство в областта на киберсигурността. ЕС ще инвестира *450 милиона евро в това партньорство, по програмата си за изследвания и иновации Хоризонт 2020*[4]. Очаква се участниците на пазара за киберсигурност, представлявани от Европейската организация за киберсигурност (ECSO), да инвестират три пъти повече. Това партньорство включва и членове на националните, регионалните и местните публични администрации, изследователските центрове и академичните среди. Целта на партньорството е да насърчава сътрудничеството на ранен етап от процеса на научни изследвания и иновации и да създаде решения за киберсигурност за различни сектори като енергетика, здравеопазване, транспорт и финанси.

Комисията също така определя различни мерки за преодоляване на фрагментирането на пазара на ЕС в областта на киберсигурността. Понастоящем на дружествата за може да се наложи да преминат различни процеси на сертифициране, за да продават своите продукти и услуги в няколко държави членки. Поради това Комисията ще разгледа евентуалното въвеждане на европейска рамка за сертифициране на продукти в сферата на информационните и комуникационните технологии (ИКТ) за сигурността. Развитието на информационните и комуникационните технологии е от жизнено важно значение за конкурентоспособността на Европа в съвременната глобална икономика с все по-силно присъствие на цифровите технологии. През периода на финансиране 2014–2020 г. за инвестиции в ИКТ са налични над 20 млрд. EUR от Европейския фонд за регионално развитие (ЕФРР)[5] и Кохезионния фонд[6].

4 http://ec.europa.eu/programmes/horizon2020/
5 http://ec.europa.eu/regional_policy/index.cfm/bg/funding/erdf/
6 http://ec.europa.eu/regional_policy/index.cfm/bg/funding/cohesion-fund/

Тези инвестиции подпомагат действията на Комисията за създаване на цифров единен пазар, който има потенциала да генерира до 250 млрд. EUR допълнителен растеж.

Огромен брой новаторски европейски малки и средни предприятия (МСП) се появиха в пазарни ниши (напр. криптиране) и в добре установени пазари с нови стопански модели (напр. антивирусен софтуер), но често не са в състояние да разрастват операциите си. Комисията иска да се улесни достъпа до финансиране за по-малките предприятия, работещи в областта на киберсигурността и ще проучи различни варианти в рамките на Инвестиционния план на ЕС.[7]

Жан-Клод Юнкер, председателят на Европейската комисия, заяви:

„Кибератаките могат да бъдат по-опасни за демократичната и икономическата стабилност от оръжията и танковете. През последните години постигнахме напредък в безопасността на европейците онлайн. Но Европа все още не е добре оборудвана срещу кибератаки. Ето защо днес Комисията предлага нови инструменти, включително европейска агенция за киберсигурност, които да ни помогнат да се защитим от тези атаки."

Мария Габриел, комисар по въпросите на цифровата икономика и цифровото общество, заяви:

„Трябва да укрепим доверието на гражданите и предприятията в света на цифровите технологии, особено в момент, когато мащабните кибератаки стават все по-често явление. Искам високи стандарти в областта на киберсигурността, които да се превърнат в новото конкурентно предимство на нашите предприятия."

Федерика Могерини, заместник-председател на Европейската Комисия и върховен представител на Съюза по въпросите на външните работи и политиката на сигурност заяви:

„ЕС ще се стреми към международна киберполитика, насърчаваща отворено, свободно и сигурно киберпространство, ще подпомага усилията за разработване на стандарти за отговорно поведение на държавите и ще прилага международното право и мерки за изграждане на доверие в областта на киберсигурността."

7 http://www.consilium.europa.eu/bg/policies/investment-plan/

Директивата за мрежова и информационна сигурност

В стратегията се прави предложение за *директива в областта на мрежовата и информационна сигурност*. Тя е важен елемент от цялостната стратегия и изисква от всички държави членки, основни доставчици на интернет и оператори на критични инфраструктури, като платформи за електронна търговия и социални мрежи, и оператори в областта на енергетиката, транспорта, банковото дело и здравните услуги да гарантират сигурна и надеждна цифрова среда в целия ЕС. Предложената директива установява мерки, които включват:

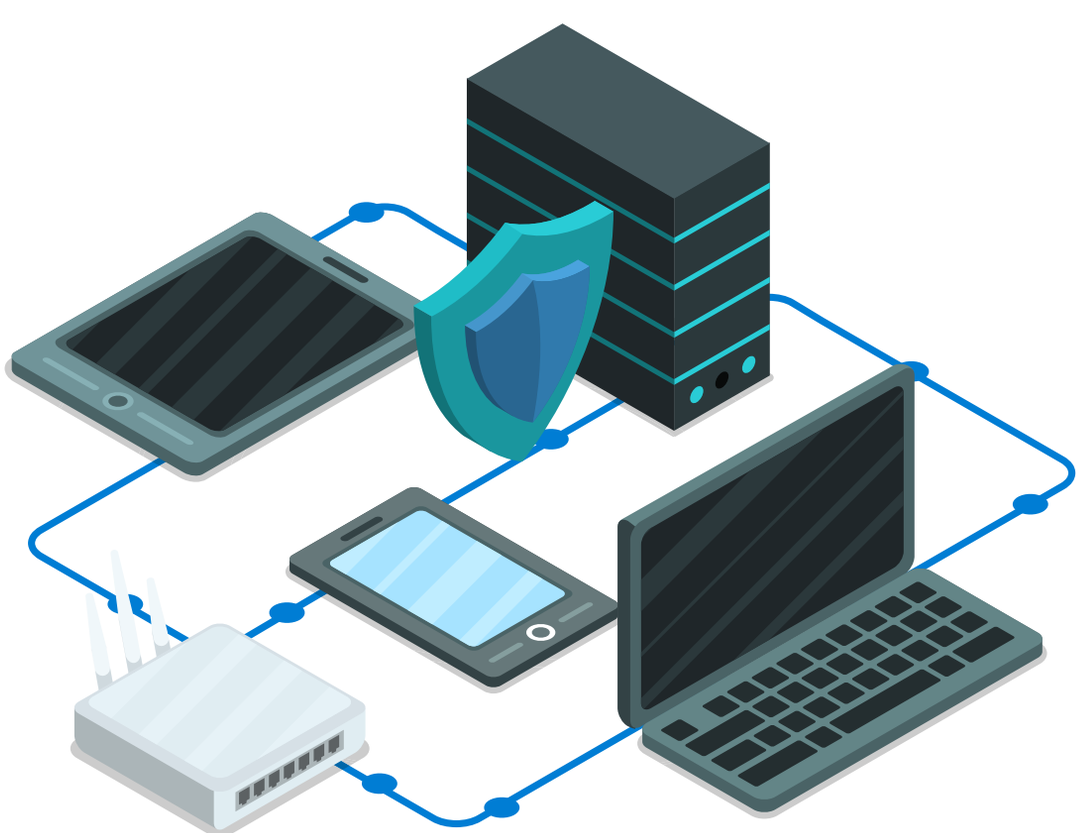
- Държавите членки трябва да приемат стратегия за киберсигурност и да определят национален компетентен орган по киберсигурност с достатъчни човешки и финансови ресурси, за да предотвратява, управлява и реагира в случай на рискове и инциденти в областта на МИС;
- Създава се механизъм за сътрудничество между държавите членки и Комисията за споделяне на ранни предупреждения за рискове и инциденти чрез сигурна инфраструктура, за сътрудничество и за организиране на редовни партньорски оценки;
- Операторите на критични инфраструктури в някои сектори (финансови услуги, транспорт, енергетика и здравеопазване), доставчиците на услуги за информационното общество (по-специално: платформи за електронна търговия с приложения, плащания по интернет, изчисления в облак, търсачки, социални мрежи) и публичните администрации трябва да въведат практики за управление на риска и да докладват значителни инциденти, свързани със сигурността на основните им услуги.

На 6 юли 2016 г. Европейският парламент одобри първият закон за киберсигурност в Европейския съюз: Директивата за мрежова и информационна сигурност (NIS)[8]. Целта на директивата е да се постигне по-високо общо ниво на сигурност на мрежовите системи и информационни в рамките на ЕС, с помощта на:

» Подобряване на възможностите за киберсигурност на национално ниво
» Подобряване на сътрудничеството на европейско равнище
» Управление на риска и задължения за докладване на инциденти към оператори на основни услуги и доставчиците на цифрови услуги

8 https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016L1148

В приветственото си изявление, заместник-председателят за Цифровия единен пазар към ЕК Андрус Ансип сподели: “Ако искаме хората и бизнеса да се възползват максимално от цифровите услуги, те трябва да им имат доверие. Цифровият единен пазар може да бъде създаден само в сигурна онлайн среда. Директивата за мрежова и информационна сигурност е първият мащабен законодателен акт на ЕС в сферата на киберсигурността и фундаментална основа за нашата работа в тази област. Той изисква от компаниите в критичните сектори, като енергетиката, транспорт, банковото дело и здравеопазване, да усвоят практики за управление на риска и да докладват за сериозни инциденти, които могат да повлияят на Цифровия единен пазар пред националните органи в въответните страни, които, от своя страна, ще могат да провеждат по-успешно изграждане на капацитет с по-голямо трансгранично сътрудничество в рамките на ЕС. Директивата задължава също онлайн магазините, cloud computing услугите и търсачките да предприемат подобни стъпки за сигурност.”



Реформа в областта на киберсигурността в Европа

Европейският съюз възнамерява да въведе по-строги правила за киберсигурност, за да води борба с нарастващите заплахи от кибератаки, както и да се възползва от възможностите на новата цифрова ера.

На заседанието си на 19 и 20 октомври 2017 г. Европейският съвет призова за приемането на общ подход към киберсигурността в ЕС като последващо действие във връзка с пакета за реформа, предложен от Европейската комисия през септември. Целта на реформата е да се доразвият мерките, въведени със стратегията за киберсигурността и нейния основен стълб – директивата за мрежовата и информационната сигурност (Директивата за МИС).

Предложението съдържа нови инициативи, например:

- изграждане на по-солидна агенция на ЕС за киберсигурността
- въвеждане на схема за сертифициране на киберсигурността на равнище ЕС
- бързо прилагане на Директивата за МИС

Лидерите от ЕС разглеждат реформата на киберсигурността като един от настоящите основни аспекти по пътя към доизграждането на цифровия единен пазар на ЕС.

ЗАЩО Е НЕОБХОДИМО ТОВА?

Изправен пред все по-сериозни предизвикателства в областта на киберсигурността, ЕС трябва да подобри осведомеността на хората и възможностите за реагиране на кибератаки, насочени срещу държавите членки или институциите на ЕС.

„Интернет на предметите“ вече е реалност, като се предвижда до 2020 г. в ЕС да има десетки милиарди свързани цифрови устройства.

Същевременно съвременните ИКТ системи могат да бъдат сериозно засегнати от свързани със сигурността инциденти като технически повреди и вируси. Този вид инциденти, често наричани инциденти, свързани с мрежовата и информационната сигурност, зачестяват все повече и стават все по-трудни за отстраняване.

Агенция на Европейския съюз за мрежова и информационна сигурност

	СЕГА	В БЪДЕЩЕ
ПЕРСОНАЛ	84 души	125 души
БЮДЖЕТ	€11 милиона	€23 милиона

Задачи, поставени пред реформираната агенция:

РАЗРАБОТВАНЕ И ПРИЛАГАНЕ НА ПОЛИТИКИ

да се засили подкрепата за Комисията и държавите-членки при разработването, прилагането и прегледа на общата политика в областта на киберсигурността и в ключови стратегически сектори, определени от директивата за МИС, напр. енергетиката, транспорта и финансите.

ЗНАНИЯ И ИНФОРМАЦИЯ

да се предоставят анализи и съвети и да се повиши осведомеността, да се превърне в едно звено за подробна информация за киберсигурността от институциите и органите на ЕС.

ИЗГРАЖДАНЕ НА ЗНАНИЯ И УМЕНИЯ

да се засили подкрепата за държавите-членки, за да се подобрят способностите и експертните знания, например относно предотвратяването и реагирането при инциденти.

ЗАДАЧИ, СВЪРЗАНИ С ПАЗАРА

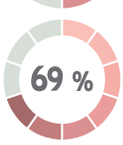
в рамките на сертификационната рамка за киберсигурността да се подготвят общоевропейски схеми за сертифициране на киберсигурността, с експертната помощ и тясното сътрудничество на националните органи за сертифициране. Схемите ще бъдат приети от Комисията.

Освен това се очаква кибератаките да струват на световната икономика 400 милиарда евро годишно.

Много предприятия и правителства в ЕС разчитат на цифрови мрежи и инфраструктура за предоставянето на основните си услуги. Това означава, че когато възникнат свързани с МИС инциденти, те могат да окажат огромно въздействие, като нарушат предоставянето на услуги и спрат нормалната работа на предприятията. Поради това свързан с МИС инцидент в една държава може да окаже въздействие в други държави и дори в целия ЕС. Свързаните със сигурността инциденти подкопават и доверието на потребителите в системите за онлайн плащания и в ИКТ мрежите.

Въпреки нарастващата заплаха, осведомеността и знанията в областта на киберсигурността все още са недостатъчни:

от европейските граждани намират, че не са запознати с кибернетичните заплахи,



от фирмите нямат елементарни познания за кибернетичния риск, на който са изложени.

За да осигури на Европа подходящите инструменти за посрещане на кибератаки, Европейската комисия и върховният представител предлагат широк набор от мерки за повишаване на киберсигурността в ЕС. Сред тях е предложението за създаване на нова агенция на ЕС за киберсигурност, която да подпомага държавите членки при посрещането на кибератаки, и за въвеждане на нова европейска схема за сертифициране, която да гарантира, че продуктите и услугите в света на цифровите технологии са безопасни за ползване.

Скорошните атаки посредством софтуер за изнудване, драстичното увеличаване на престъпната дейност в киберпространството, нарастващото използване на киберинструменти от страна на държавни участници за постигане на геополитическите им цели и диверсификацията на инцидентите с киберсигурността обосновават необходимостта ЕС да изгради по-силна устойчивост на кибератаките и да създаде ефективен механизъм за кибервъзпиране и за отговор с наказателноправни средства на кибератаките, за да бъдат по-добре защитени европейските граждани, предприятия и публични институции. Днешният пакет от мерки в областта на киберсигурността третира именно тези въпроси.

ИЗГРАЖДАНЕ НА УСТОЙЧИВОСТТА НА ЕС: СИЛНА АГЕНЦИЯ НА ЕС ЗА КИБЕРСИГУРНОСТ

Като се използва опита на съществуващата *Агенция на Европейския съюз за мрежова и информационна сигурност (ENISA)*, на новата *Агенция на ЕС за киберсигурност:* ще бъде предоставен постоянен мандат да подпомага държавите членки при предприемането на ефективни мерки за предотвратяване на кибератаки и за противодействието им. Агенцията ще подобри готовността на ЕС за реакция, като организира годишни общоевропейски учения по киберсигурност и като осигурява по-добър обмен на знания и информация за заплахи чрез създаването на центрове за обмен и анализ на информация. Това ще подпомогне прилагането на Директива за мрежова и информационна сигурност, в която са предвидени задължения за националните органи да докладват в случай на сериозни инциденти.

Агенцията за киберсигурност също така ще помогне за въвеждането и прилагането на общоевропейска нормативна уредба за сертифициране, предложена от Комисията с цел гарантиране на съответствие на продуктите и услугите с изискванията за киберсигурност. По същия начин, по който етикетите на храните дават на потребителите надеждност относно това, което консумират, новите европейски сертификати за киберсигурност ще осигурят надеждността на милиарди устройства („интернет на нещата“), които са в основата на съвременните критични инфраструктури, като енергийните и транспортните мрежи, но също и новите потребителски устройства, като например свързаните автомобили. Сертификатите за киберсигурност ще се признават във всички държави членки, което ще доведе до намаление на административната тежест и цените за дружествата.

ЗАСИЛВАНЕ НА КАПАЦИТЕТА НА ЕС В ОБЛАСТТА НА КИБЕРСИГУРНОСТТА

ЕС има стратегически интерес да гарантира, че технологичните инструменти за гарантиране на киберсигурността се разработват по начин, който позволява на цифровата икономика да се развива, като същевременно се защитават сигурността, обществото и демокрацията ни. За да се засили капацитетът на ЕС в областта на киберсигурността, Комисията и върховният представител на Съюза по въпросите на външните работи и политиката на сигурност предлагат: *Европейски експертен център за научни изследвания в областта на киберсигурността* (през 2018 г. предстои стартирането на пилотен проект). В сътрудничество с държавите членки той ще спомогне за разработването и въвеждането на инструментите и технологиите, необходими, за да сме в крак с непрестанно променящата се заплаха и да гарантираме, че нашите защитни механизми са също толкова съвременни от технологична гледна точка, колкото и използваните от киберпрестъпниците средства. Центърът ще допълва усилията за изграждане на *капацитет* в тази област на равнище ЕС и на национално равнище.

Концепция за начина, по който Европа и държавите членки могат да реагират бързо, оперативно и в унисон, когато започне мащабна кибератака. Предложената процедура е установена в препоръка. Препоръката също така призовава държавите членки и институциите на ЕС да създадат механизъм на ЕС за реакция при кризи в областта на киберсигурността, за да приведат концепцията в действие. Процедурата ще бъде редовно изпитвана по време на учения по управление на киберкризи и други кризи.

Повече солидарност: В бъдеще би могла да се разгледа възможността за създаване на нов фонд за реакция при спешни случаи в областта на киберсигурността в полза на тези държави членки, които отговорно са изпълнили всички мерки за киберсигурност, изисквани съгласно правото на ЕС. Фондът би могъл да предоставя спешна подкрепа в помощ на държавите членки — по същия начин, по който механизмът на ЕС за гражданска защита се използва за предоставяне на помощ при случаи на горски пожари или природни бедствия.

Засилване на способностите за киберотбрана: Държавите членки се насърчават да включат киберотбраната в рамките на постоянното структурирано сътрудничество и на Европейския фонд за отбрана, за да бъдат подпомагани проектите в областта на киберотбраната. Европейският експертен център за научни изследвания в областта на киберсигурността би могъл също да бъде допълнен с измерение, свързано с киберотбраната. За да бъде преодолян недостигът на умения в областта на киберотбраната, през 2018 г. ЕС ще създаде платформа за обучение и образование в областта на киберотбраната. ЕС и НАТО заедно ще насърчават сътрудничеството

в областта на научните изследвания и иновациите, свързани с киберотбраната. Ще бъде задълбочено сътрудничеството с НАТО, включително участието в паралелни и координирани учения.

Засилено международно сътрудничество: ЕС ще засили реакцията си на кибератаки чрез прилагане на Рамката за съвместен дипломатически отговор на ЕС на злонамерените дейности в киберпространството и чрез подкрепа за стратегическа рамка за предотвратяване на конфликти и за стабилност в киберпространството. Това ще бъде придружено от нови усилия за изграждане на киберкапацитет с цел подпомагане на трети държави при справянето с киберзаплахи.

ПРЕДПРИЕМАНЕ НА ЕФЕКТИВНИ НАКАЗАТЕЛНОПРАВНИ МЕРКИ

Предприемането на по-ефективни мерки в областта на правоприлагането, насочени към откриване, проследяване и наказателно преследване на киберпрестъпниците, е от основно значение за създаването на силно възпиращо действие срещу извършването на киберпрестъпления. Ето защо Комисията предлага да се засили възпиращият ефект чрез нови мерки за борба с измамата и подправянето на непарични платежни средства.

Предложението за директива ще засили възможностите на правоприлагащите органи за противодействие на този вид престъпност чрез разширяване на обхвата на съставите на престъпленията, свързани с информационни системи, за да бъдат включени в него всички платежни трансакции, включително трансакциите чрез виртуални валути. Чрез законодателния акт също така ще бъдат въведени общи правила относно размера на наказанията и ще бъде изяснен обхвата на компетентността на държавите членки по такива престъпления.

За да се засили ефективното разследване и наказателно преследване на престъпления, извършвани чрез кибернетични средства Комисията ще представи предложения за улесняване на трансграничния достъп до цифрови доказателства. Освен това до октомври Комисията също така ще представи своите размисли във връзка с ролята на криптирането в наказателните разследвания.

УКРЕПВАНЕ НА МЕЖДУНАРОДНОТО СЪТРУДНИЧЕСТВО В СФЕРАТА НА КИБЕРСИГУРНОСТТА

Ръководена от основните ценности и права като свобода на изразяване, право на неприкосновеност на личния живот и защита на личните данни, и утвърждаването на открито, свободно и сигурно киберпространството, политиката на ЕС за международна киберсигурност има за цел да отговори на постоянно развиващото се предизвикателство да се поддържа стабилност на световното киберпространство и да допринесе за стратегическата независимост на Европа в киберпространството.

Рамка на ЕС за сертифициране на киберсигурността

Сертифицирането играе ключова роля за повишаване на доверието и сигурността на продуктите и услугите, които са от решаващо значение за единния цифров пазар. В момента в ЕС съществуват редица различни схеми за сертифициране на сигурността на продуктите от ИКТ.

СЪЩЕСТВУВАЩИТЕ СЕРТИФИКАЦИОННИ СХЕМИ В ЕС

Понастоящем в Европа има съвкупност от схеми и инициативи за сертифициране на киберсигурността, но националните инициативи за сертифициране вече са въведени или се появяват, без да се признават взаимно.

Осигурената в Обединеното кралство *търговска продуктова гаранция* се прилага за търговски продукти, на които се издава сертификат, който доказва задоволителна търговска сигурност и удостоверява, че даден продукт е с ниско ниво на заплаха. Въпреки това, няма споразумение за взаимно признаване на сертификатите, което означава, че продуктите, тествани в Обединеното кралство, не биха били приети като сертифицирани продукти на други пазари.

Sécuritaire de Premier Niveau (CSPN) е схема за сертифициране, създадена от Френската агенция за мрежова и информационна сигурност (ANSSI). Схемата е разработена като по-лека алтернатива на CC сертификациите. За нея също липсва общоевропейско споразумение за взаимно признаване.

Холандската схема за оценка на продуктите за сигурност[9] предоставя информация за пригодността на продуктите за ИТ сигурност за използване в "чувствителния, но некласифициран" домейн. Схемата на БДЗП е в пилотна фаза от 2015 г.

SOG-IS MRA включва 12 държави-членки плюс Норвегия. В рамките на инициативата са разработени няколко профила за защита на цифрови продукти, напр. цифров подпис, цифров тахограф и смарт карти. Членовете могат да участват в споразумение за взаимно признаване като сертификат за потребителите и производителите.

9 Baseline Security Product Assessment (BSPA)

Фактите сочат, че хората във всички части на света определят кибератаките от други държави за една от най-важните заплахи за националната сигурност. При глобалния характер на заплахите изграждането и поддържането на здрави съюзи и партньорства с трети държави има основно значение за предотвратяването и възпирането на кибератаки, които влияят все повече върху международната стабилност и сигурност. ЕС ще счита създаването на стратегическа рамка за предотвратяване на конфликти и за стабилност в киберпространството за приоритет в своите двустранни, регионални, многостранни ангажименти и в ангажиментите си с много на брой заинтересовани страни.

ЕС силно подкрепя становището, че международното право и по-специално Хартата на ООН, е в сила и в киберпространството. Като допълнение към задължителните международни правни норми ЕС подкрепя доброволните незадължителни норми, правила и принципи за отговорно държавно поведение, формулирани от групата правителствени експерти към ООН, освен това Съюзът насърчава разработването и прилагането на регионални мерки за изграждане на доверие, както в рамките на Организацията за сигурност и сътрудничество в Европа, така и в други региони. На двустранно равнище диалогът относно киберсигурността ще бъде допълнително развит и допълнен от усилия за улесняване на сътрудничеството с трети държави за укрепване на принципите на надлежни проверки и държавна отговорност в киберпространството. ЕС ще счита въпросите на международната сигурност в киберпространството за приоритет в своите международни ангажименти, същевременно обръщайки внимание киберсигурността да не се превръща в претекст за протекция на пазари и ограничаване на основни права и свободи, включително свобода на изразяване и достъп до информация. Комплексният подход към киберсигурността изисква зачитане на правата на човека и ЕС ще продължи да подкрепя основните ценности на Съюза в световен мащаб, доразвивайки своите насоки относно правата на човека за свободата в интернет. В това отношение Съюзът подчертава значението на участието на всички заинтересовани страни в управлението на интернет. Освен това Комисията представи предложение за модернизиране на контрола на ЕС върху износа, включително въвеждане на контрол върху износа на критични технологии за кибернаблюдение, които могат да причинят нарушения на човешките права или с тях да се злоупотреби срещу собствената сигурност на ЕС, и ще развива диалога с трети държави за насърчаване на глобално сближаване и отговорно поведение в тази област.

Глобалната стабилност в киберпространството разчита на местната и националната способност на всички държави да предотвратяват и да реагират на киберинциденти, и да разследват и съдебно да преследват случаите на киберпрестъпления. Подпомагането на усилията за изграждане на устойчивост в трети държави ще увеличи равнището на киберсигурността в глобален мащаб, а това ще има положителни последици за ЕС.

Противодействието на бързо развиващите се киберзаплахи е свързано с необходимост от действия за обучение, за разработване на политики и законодателство, както и от ефективно функциониращи екипи за незабавно реагиране при компютърни инциденти и звена за борба с киберпрестъпленията във всички държави в света.

От 2013 г. ЕС е лидер в изграждането на международен капацитет за киберсигурност и систематично свързва тези усилия със сътрудничеството за развитие. ЕС ще продължи да насърчава модел на изграждане на капацитет, основан на правата, в съответствие с подхода Digital4Development (цифрови технологии за развитие).

Приоритетите за изграждане на капацитет ще са съседните на ЕС държави и развиващите се държави, в които свързаността нараства бързо и заплахите се развиват с висока скорост. Усилията на Съюза ще допълват програмата на ЕС за развитие в светлината на Програмата за устойчиво развитие до 2030 г. и цялостните действия за изграждане на институционален капацитет.

За подобряване на способността на ЕС да мобилизира своите колективни експертни знания и опит в помощ на изграждането на такъв капацитет следва да се създаде специална мрежа на ЕС за изграждане на киберкапацитет, обединяваща Европейска служба за външна дейност (ЕСВД)[10], органите на държавите членки, отговарящи за киберпространството, агенции на ЕС, службите на Комисията, академичните институции и гражданското общество. Ще бъдат разработени насоки на ЕС за изграждане на киберкапацитет, които ще спомогнат за по- добро политическо ръководство и определяне на приоритети на действията на ЕС за подпомагане на трети държави.

Също така ЕС ще работи съвместно с други донори в тази област, за да се избегне дублирането на усилията и да се съдейства за по-целенасочено изграждане на капацитет в различните региони.

10 https://europa.eu/european-union/about-eu/institutions-bodies/eeas_bg

СЪТРУДНИЧЕСТВО МЕЖДУ ЕС И НАТО

Надграждайки съществения напредък, който вече е постигнат, ЕС ще задълбочава сътрудничеството с НАТО в областта на киберсигурността, хибридните заплахи и отбраната, както предвижда съвместната декларация от 8 юли 2016 г. Приоритетите включват насърчаване на оперативната съвместимост чрез ясни изисквания и стандарти, засилване на сътрудничеството при обучение и учения, хармонизиране на изискванията за обучение.

ЕС и НАТО ще подпомагат също и сътрудничеството в научните изследвания и иновации за киберотбраната и ще развиват съществуващото техническо споразумение за обмен на информация относно киберсигурността между техните съответни органи по киберсигурност. Неотдавнашните съвместни постижения за противодействие на хибридните заплахи, по-специално сътрудничеството между Звеното на ЕС за синтез на информацията за хибридните заплахи и клона, създаден в рамките на НАТО за анализ на хибридните заплахи, следва да се развиват допълнително за засилване на устойчивостта и по-успешно реагиране при киберкризи. По-нататъшното сътрудничество между ЕС и НАТО ще се подпомага чрез учения за киберотбрана с участието на ЕСВД и други органи на ЕС и съответните органи на НАТО, включително Съвместният експертен център на НАТО за кибернетична защита, разположен в Талин.

За пръв път НАТО и ЕС ще проведат успоредни и координирани учения за реагиране на сценарии за хибридна заплаха, като НАТО ще води учението през 2017 г., а през 2018 г. ЕС на свой ред ще поеме водеща роля. Следващият доклад относно сътрудничеството между ЕС и НАТО ще предложи да се разгледат възможностите за по-нататъшно разширяване на сътрудничеството, по-специално чрез осигуряване на общи, сигурни и надеждни начини за комуникация между всички участващи съответни институции, включително ENISA.

КЛЮЧОВИ ДЕЙСТВИЯ:

- Осъществяване на напредък по стратегическата рамка за предотвратяване на конфликти и за стабилност в киберпространството;
- Създаване на нова мрежа за изграждане на капацитет за подпомагане на способността на трети държави да се справят с киберзаплахи, и разработване на насоки на ЕС за изграждане на киберкапацитет, за да се определят по-успешно приоритетите в усилията на Съюза;
- По-нататъшно сътрудничество между ЕС и НАТО, включително участие в успоредни и координирани учения и по-добра оперативна съвместимост на стандартите за киберсигурност.

В своя пакет за реформа от септември 2017 г. Европейската комисия предложи въвеждането на схеми за сертифициране на ИКТ продукти, услуги и процеси на равнище ЕС. Целта на тази инициатива е да се даде възможност за растеж на пазара на ЕС в областта на киберсигурността.

Схемите за сертифициране ще бъдат под формата на правила, технически изисквания и процедури. Чрез тях ще се намали фрагментираността на пазара и ще се премахнат регулаторните пречки, като същевременно ще се изгради доверие. Те ще бъдат признати във всички държави членки, което ще улесни трансграничната търговия за предприятията.

Развитието на пазара на решения, свързани с киберсигурността в ЕС — по отношение на продукти, услуги и процеси — среща трудности по няколко основни причини. Основен аспект е липсата на схеми за сертифициране за киберсигурност, признати в целия ЕС, за вграждане в продуктите на по-високи стандарти за устойчивост и укрепване на доверието към пазара в целия ЕС. Затова Комисията предлага да се създаде *европейска рамка за сертифициране за киберсигурност.* Агенцията за кибернетична сигурност, ENISA, ще въведе и прилага този процес на сертифициране. Предложената рамка за сертифициране в целия ЕС създава всеобхватен набор от правила, технически изисквания, стандарти и процедури за съгласуване на всяка схема. Всяка схема ще се основава на споразумение на равнище ЕС за оценка на свойствата на сигурността на конкретен продукт или услуга, базирани на ИКТ. Това удостоверение ще удостоверява, че продуктите и услугите на ИКТ, които са сертифицирани в съответствие с такава схема, отговарят на определени изисквания за киберсигурност. Полученият сертификат ще бъде признат във всички държави-членки.

Рамката ще донесе определени ползи за бизнеса чрез премахване на необходимостта да се преминава през няколко процедури за сертифициране при търговия зад граница и по този начин ще намали административните и финансовите разходи. Освен това използването на схеми, разработени в тази рамка, ще спомогне за изграждане на доверие у потребителите, като сертификат за съответствие ще уведомява и уверява купувачите и потребителите относно свързаните със сигурността свойства на продуктите и услугите, които те купуват и използват. Това ще направи високите стандарти за киберсигурност източник на конкурентно предимство. В резултат ще се повиши устойчивостта, тъй като изделията и услугите в областта на ИКТ официално ще се оценяват спрямо определени стандарти за киберсигурност, които могат да бъдат разработени в тясна връзка с продължаващата по-широка работа по стандартите в сферата на ИКТ.

КОЙ ЩЕ СЕ ВЪЗПОЛЗВА ОТ РАМКАТА ЗА СЕРТИФИЦИРАНЕ И ПО КАКЪВ НАЧИН?

Способността да се разбере дали даден продукт, система или услуга отговаря на определени изисквания е в основата на доверието в цифровите системи или устройства, които използваме. Поради това рамката ще е от полза за:

- Граждани и крайни потребители (например оператори на основни услуги), които ще могат да правят по-информиран избор за покупка на продукти и услуги в областта на ИКТ, които използват в ежедневието си.

- Продавачи и доставчици на продукти и услуги в областта на ИКТ (включително МСП и нови предприятия). Те ще трябва да преминат през единна процедура, за да получат европейски сертификат, валиден във всички държави членки. За МСП и нови предприятия това също така ще означава премахване на евентуални бариери за навлизане на пазара. Като избягват необходимостта от преминаване през няколко процедури на сертифициране, разходите за които могат да се различават значително в зависимост от продукта/услугата, търсената оценка на нивото на надеждност и други елементи, предприятията ще спестят много средства. Така например разходите за сертификата „Портал за интелигентни измервателни уреди“ на Федералната служба за сигурност на информационните технологии на Германия (BSI) надхвърлят 1 млн. евро (най-високото равнище на изпитване и надеждност, отнася се не само до продукта, но и до цялата свързана с него инфраструктура), докато разходите за сертифициране на интелигентни измервателни уреди в Обединеното кралство и Франция са около 150 000 евро. Накрая, тъй като се очаква търсенето на по-сигурни решения да нарасне в световен мащаб, продавачите и доставчиците също ще се ползват с конкурентно предимство за задоволяване на тези потребности.

- Правителствата също ще могат да вземат по-информирани решения за покупки и в същото време ще разполагат с институционална рамка, която им дава възможност да откриват и посочват приоритетни области, нуждаещи се от сертифициране по отношение на сигурността в областта на ИКТ.

Сред мерките, изтъкнати от Съвета, са предоставянето на необходимите инструменти за правоприлагане за противодействие на киберпрестъпността, разработването на координирана реакция на равнището на ЕС на мащабни кибернетични инциденти и кризи и редовното провеждане на паневропейски учения за киберсигурност. Във връзка с глобалните и дипломатическите аспекти на киберсигурността Съветът признава значението на международното сътрудничество и приветства създаването на ясна рамка за използването на политическите, дипломатическите и икономическите инструменти, с които ЕС разполага, като реакция на злонамерени действия в киберпространството.

ОТ ПОДКРЕПА ЗА КОМПЕТЕНЦИИТЕ ДО БОРБА С ИЗМАМИТЕ

Предложението на Европейската комисия за укрепване на киберсигурността в ЕС включва и допълнителни инициативи:

» концепция за начина на реагиране на мащабни кибератаки

» Европейски експертен център за научни изследвания в областта на киберсигурността наред с мрежа от подобни центрове на равнище държави членки

» по-ефективно противодействие на киберпрестъпността със средствата на наказателното право чрез нова директива за борба срещу измамите и фалшифицирането на непарични платежни средства

» укрепване на стабилността в глобален мащаб чрез международно сътрудничество.

В Съвета

На 24 октомври 2017 г. Съветът по телекомуникации постигна съгласие за създаването на план за действие за реформата на ЕС в областта на киберсигурността. Министрите подчертаха, че онлайн сигурността е от съществено значение за европейските граждани и предприятия.

На 20 ноември Съветът по общи въпроси призова за укрепване на киберсигурността в Европа и за повишаване на устойчивостта на киберпространството в ЕС. Тези цели съответстват на приоритетите, определени от Европейския съвет през октомври 2017 г. Министрите подчертаха потребността всички страни от ЕС да осигурят необходимите ресурси и инвестиции за решаване на въпроса за киберсигурността. Те изтъкнаха и важната връзка между доверието в цифрова Европа и постигането на устойчивост на киберпространството в целия ЕС.

В заключенията се подчертава потребността всички страни от ЕС да осигурят необходимите ресурси и инвестиции за справяне с предизвикателствата пред киберсигурността. Те приветстват намерението за увеличаване на усилията на ЕС в областта на свързаните с киберсигурността научни изследвания и развойна дейност посредством създаването на мрежа от центрове за компетентност относно киберсигурността в целия Съюз.

Освен това Съветът подкрепя плана за създаване на европейска рамка от световна класа за сертифициране на киберсигурността с цел повишаване на доверието в цифровите решения. В заключенията се изтъква важната връзка между доверието в цифрова Европа и постигането на устойчивост на киберпространството в целия ЕС. Съществено внимание се отделя на мощта на криптографията, използвана при продукти и услуги в рамките на цифровия единен пазар.

Цифровият единен пазар е сред първостепенните приоритети на Комисията „Юнкер“. Напълно функциониращият цифров единен пазар би могъл да допринесе с 415 млрд. евро годишно към икономиката и да създаде стотици хиляди нови работни места. Само две години след като започна изграждането му, ЕС успя да постигне важни договорености за премахване на таксите за роуминг от 15 юни 2017 г. за всички пътуващи в ЕС, за преносимост на съдържанието, благодарение на която от началото на 2018 г. европейците при пътуване ще могат да ползват филмите, музиката и видеоигрите или електронните книги, за които имат абонамент в родните си страни, и за освобождаването на радиочестотната лента около 700 MHz, за да се въведат мрежи от пето поколение и нови онлайн услуги. По останалите предложения понастоящем се водят заключителни преговори с Европейския парламент и Съвета.

В съответствие с обявеното в стратегията за цифровия единен пазар Европейската комисия е внесла от май 2015 г. до сега 35 законодателни предложения и политически

инициативи. В момента вниманието е съсредоточено върху това да се постигне политически консенсус с Европейския парламент и Съвета по всички предложения и най-вече по актуализираните правила на ЕС в областта на далекосъобщенията, за да се стимулират инвестициите във високоскоростни и качествени мрежи, които са от решаващо значение за пълната реализация на цифровата икономика и цифровото общество е немислима.

Цифров единен пазар

ОСИГУРЯВАНЕ НА СИГУРНОСТ ЗА ЦИФРОВИЯ ЕДИНЕН ПАЗАР

Киберсигурността може да открие възможности за иновации и да спомогне за насочване на вниманието към данните в качеството им на ново „гориво за икономиката“. Да се осигури цифрово бъдеще за Европа означава също:

- да се води борба със заплахите пред онлайн платформите и да им се даде възможност за положителен принос към обществото
- да се оказва съдействие на малките и средните предприятия, за да бъдат конкурентоспособни в условията на цифровата икономика
- да се инвестира в използването на изкуствения интелект и суперкомпютрите в области като медицинското лечение и енергийната ефективност.

По данни проучване Евробарометър две трети от европейците са на мнение, че използването на най-новите цифрови технологии оказва положително въздействие върху обществото, икономиката и техния собствен живот. Повечето от отговорилите очакват ЕС, държавите членки и предприятията да предприемат действия, за да се справят с проблемите, които поражда цифровизацията (например въздействието върху работните места и нуждата от по-добри цифрови умения).

По-съществените кибер атаки през 2016 и 2017

ДЕКЕМВРИ 2015-ДЕКЕМВРИ 2016

Електрическата мрежа в Украйна

230 000 души бяха оставени без електричество за над 6ч. отбелязвайки първият официален случай, в който кибероръжие се използва за атака на национална електроснабдителна мрежа.

ОКТОМВРИ 2016

Австралийския червен кръст

Личните данни на 550 000 кръвни донори са откраднати.

НОЕМВРИ 2016

Yahoo

Компроментиране на информация на над 1 000 000 акаунта.

ОКТОМВРИ 2016

Демократичният национален комитет

20 000 имейла са откраднати.

НОЕМВРИ 2016

Дойче Телеком

900 000 са пострадалите от прекъсване на интернет връзката за период от два дни.

ФЕВРУАРИ 2016

ФБР

Личните данни на 20 000 служители на ФБР са изтекли.

АПРИЛ 2016

Доставчика на домейни Дин

Атака довежда до пробив в някой от най-големите сайтове на света: Twitter, Netflix, Reddit, CNN, The Guardian.

АПРИЛ 2016

Филипинската изборна комисия

Личните данни на всички избиратели във Филипините са компроментирани от Анонимните. Засегнати са около 55 миниона души.

По-съществените кибер атаки през 2016 и 2017

АПРИЛ 2017
Изтичане на правителствена информация

Компроментирани са редица сервъри на Windows.

МАЙ 2017
WannaCry

Над 300 хил. компютри са били засегнати в редица индустрии.

ЮНИ 2017
Данни за гласуване

Данните на над 200 млн. гласоподаватели са разкрити.

ЮНИ 2017
Petya

Компютърния вирус Petya, води до загуби в размер на 300 млн. долара

ОКТОМВРИ 2017
Bad Rabbit

Атаката е засегнала предимно потребители от Русия, Украйна и Турция.

МАРТ 2017
UBER

Хакери откраднат данните на над 57 млн. потребители на UBER.

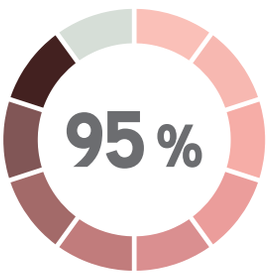
НОЕМВРИ 2016
Tesco Bank

Откраднати са над 2 500 000 лири от около 9000 потребителя с този хак.

ФЕВРУАРИ 2016
Централната банка на Бангладеш

$81 000 000 са загубени, а загубата на $850 000 000 е предотвратена чрез прекъсване на транзакциите.

Насърчаване на кибернетичната хигиена и осведоменост



Отчита се, че около 95 % от инцидентите са станали възможни поради „*някакъв вид човешка грешка, съзнателна или несъзнателна*“, това е показателно за силната роля на човешкия фактор. Следователно киберсигурността отговорност на всеки човек. Това означава, че личното поведение, поведението в корпоративен план и това на публичната администрация трябва да се променят, за да се гарантира, че всеки човек разбира опасността и разполага с необходимите средства и умения бързо да открива атаки и активно да се защити от тях. Нужно е хората да си създадат навици за кибернетична хигиена, а бизнесът и организациите трябва да приемат подходящи програми за киберсигурност, основани на рисковете, и периодично да ги актуализират, за да отразяват развиващата се ситуация на рискове.

Директивата за МИС определя отговорностите на държавите членки не само за обмен на информация за кибератаки на равнище ЕС, но и за въвеждане на комплексни национални стратегии и рамки за сигурност на мрежата и информационните системи.

Публичните администрации на европейско и на национално равнище трябва да изпълняват по-нататъшна водеща роля за напредък на тези действия. На първо място държавите членки следва да осигурят инструменти за киберсигурност, които да са на разположение на предприятията и хората в максимална степен. По-специално следва да се направи повече за предотвратяване на киберпрестъпленията и смекчаване на тяхното въздействие върху крайните потребители. Вече има пример в работата на Европол с кампанията „NoMoreRansom“, осъществена чрез тясно сътрудничество между правоприлагащи органи и компании за киберсигурност, за да помогне на потребителите да предотвратят заразяване със софтуер за изнудване и да декриптират данни в случай, че са станали жертва на атака. Такива схеми следва да се въведат и за други видове зловреден софтуер, в други сфери, а ЕС да разработи един портал, обединяващ всички такива инструменти на едно място, който да предлага за потребителите съвети относно предотвратяването и откриването на зловреден софтуер, както и линкове към механизми за съобщаване за такъв софтуер.

На второ място държавите членки следва да ускорят използването на по-сигурни инструменти при разработване на електронното управление и също

максимално да се възползват от мрежата за компетентност. Следва да се насърчава въвеждането на сигурни средства за идентификация, като се използва за основа рамката на ЕС.

ALLIANCE OF LIBERALS AND DEMOCRATS FOR EUROPE

Основан през 1976 г. преди първите европейски избори, алиансът става първата транснационална политическа партия през 1993 г. Партията АЛДЕ осъществява все по -жизненоважната връзка между гражданите и институциите и продължава да расте по своя размер и значимост.

АЛДЕ стои за един по-силен и по-стабилен Европейски съюз, който разполага с необходимите средства, за да отговори на безпокойствата на гражданите на Европа, свързани със сериозните проблеми, с които държавите членки не могат да се справят сами. ЕС трябва да доизгради своя вътрешен пазар в областта на енергетиката и цифровите услуги, като същевременно използва капиталовите пазари, за да помогне за финансирането на новата инфраструктура, която ще бъде в основата на икономиката на Съюза през идните години и ще създаде нови и устойчиви работни места. Според принципите на АЛДЕ Европа трябва да остане вярна и на своите ценности и да утвърждава основните права – свобода, равенство и недискриминация, необходимо е да се извърши промяна на институционално равнище, като сложи край на разхищаването на средства и започне да функционира по-ефикасно.

Усилията на групата на АЛДЕ в Европейския парламент са насочени към защита на човешките права в рамките на Европейския съюз, към превенция на рискът от ксенофобия, расизъм и антисемитизъм или хомофобия в държавите-членки, държавите-кандидатки за членство, и към състоянието на човешките права в останалата част на света. АЛДЕ се стреми

Ги Верхофстад (Белгия)
Председател на групата на ALDE

Ханс Ван Баален (Холандия)
Председател на партията на АЛДЕ

за Европа, която достига до всички европейски страни, които спазват принципите на демокрацията, върховенството на закона, човешките права и пазарната икономика. АЛДЕ е за Европа, която стимулира икономиката и създава работни места.

Групата на АЛДЕ в Европейския парламент подкрепя предприетите мерки за борба срещу киберпрестъпността. Същевременно поставя акцент върху значимостта на развитието на дигиталния единен пазар и създаването на нови възможности за бизнеса, гражданите, обществените органи и потребителите посредством усвояването на дигитални компетентности и използването на средствата, които дигиталната ера предлага. Либералите от АЛДЕ определят като една от главните си битки за този законодателен мандат поставянето на Европа в позицията на лидер в дигиталната икономика. Групата се ангажира да предприеме необходимите действия в тази посока, основавайки се на няколко основни фактора.

За да се постигне този дигитален напредък обаче, потребителите трябва да се чувстват подсигурени в кибер средата и да знаят какви са техните права, когато купуват онлайн продукт например, как да ги упражняват и какви средства за правна защита съществуват. Бизнесът също се нуждае от интелигентни, стабилни и актуални закони, които им позволяват да търгуват безопасно в бързо развиваща се среда. Така АЛДЕ приоритизира създаването на нормативна уредба, която да подсигурява безопасната дигитална търговия, правата на потребителите, авторските права в интернет, предприемане на мерки за подсигуряване на мрежова и информационна сигурност. Депутатите от АЛДЕ целят постигането на задоволително ниво на оперативно сътрудничество между държавите-членки, както и мерки за справяне с нови форми на атаки срещу мобилни плащания, електронни сметки и включването на киберсигурността в приоритетите на ЕС в областта на външните работи, за да се повиши способността на ЕС за защита от бъдещи кибератаки, а и да подобри възможността за предотвратяването на подобни бъдещи атаки. Основното притеснение на АЛДЕ в тази връзка се основава на факта, че към момента все още държавите-членки имат много различни нива на готовност да реагират на кибернетичното нападение, което води до неравностойна степен на защита на потребителите и предприятията и подкопава цялостното равнище на сигурност на Съюза.

Използвани термини и съкращения:

ЕС - Европейски съюз

Комисията „Юнкер“ - краткото название на действащата от 1 ноември 2014 г. Европейска комисия с мандат до 2019. Неин председател е Жан-Клод Юнкер, а членове са 27 комисари.

ИКТ - Информационни и комуникационни технологии

МИС - мрежовата и информационна сигурност

ECSO - Европейската организация за киберсигурност

ЕФРР - Европейския фонд за регионално развитие

МСП - малки и средни предприятия

ЕСВД - Европейска служба за външна дейност

ENISA - Агенцията за кибернетична сигурност

ОПСО - обща политика за сигурност и отбрана

НАТО - (англ. North Atlantic Treaty Organization, NATO) е международна организация за военно сътрудничество, основана с подписването на Северноатлантическия договор на 4 април 1949 г.

Това издание се реализира по инициатива на
Искра Михайлова, с
финансовата подкрепа на групата на АЛДЕ.

София,
2018

ALLIANCE OF LIBERALS AND DEMOCRATS FOR EUROPE