Нова стратегия на ЕС за киберсигурност и нови правила за повишаване на устойчивостта на физическите и цифровите особено важни субекти

Брюксел, 16 декември 2020 г.

Днес Комисията и Върховният представител на Съюза по въпросите на външните работи и политиката на сигурност представят нова стратегия на ЕС за киберсигурност. Като ключов елемент от Изграждането на цифровото бъдеще на Европа, Плана за възстановяване на Европа и Стратегията на ЕС за Съюза на сигурност, стратегията ще подкрепи колективната устойчивост срещу киберзаплахи и ще гарантира, че всички граждани и предприятия могат пълноценно да се възползват от надеждни и сигурни услуги и цифрови инструменти. Независимо дали става дума за свързани устройства, електроенергийната мрежа или банките, самолетите, публичните администрации и болниците, които европейците използват или посещават, те заслужават да правят това, като са сигурни, че са защитени от киберзаплахи.

Новата стратегия за киберсигурност позволява на ЕС освен това да утвърди водещата си роля по отношение на международните норми и стандарти в киберпространството и да засили сътрудничеството с партньори по света за насърчаване на глобално, отворено, стабилно и сигурно киберпространството основано на първенството на правото, човешките права, основните свободи и демократичните ценности

Освен това, комисията прави предложения за справяне с проблемите на кибернетичната и физическата устойчивост на особено важните субекти: Директивата за мерки на високо ниво на киберсигурността в целия Съюз и (Преработената директива за МИС или „МИС 2“) и нова директива за устойчивостта на особено важните субекти. Те обхващат широк спектър от сектори и имат за цел да се справят с настоящите и бъдещите онлайн и офлайн рискове, от кибератаките и престъпленията до природните бедствия по съгласуван и допълващ се начин.

Доверието и сигурността — в основата на „Цифровото десетилетие“ на ЕС

Новата стратегия за киберсигурност има за цел да гарантира глобален и отворен интернет, като същевременно предлага ограничения, не само за да гарантира сигурността, но и за да защитава европейските ценности и основните права на всеки гражданин. Като се основава на тези постижения от последните месеци и години, стратегията съдържат конкретни предложения за регулаторни, инвестиционни и политически инициативи в три области на действие на ЕС:

1. **Устойчивост, технологичен суверенитет и лидерство**

В контекста на тези действия Комисията предлага да се реформират правилата за сигурността на мрежите и информационните системи в рамките на директива относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (преразгледаната Директива за МИС или „МИС 2“), за да се увеличи нивото на киберустойчивост на критичните публични и частни сектори: болниците, енергийните мрежи, железниците, но също така центровете за данни, публичните администрации, научноизследователските лаборатории и производството на медицински изделия и лекарства от критично значение трябва да бъдат непробиваеми, при това в непрекъснато изменяща се и сложна обстановка, изобилстваща от заплахи.

Комисията препоръчва също така да се изгради мрежа от центрове за операции за сигурност в целия ЕС, основана на изкуствения интелект (ИИ), която да представлява истински „щит за киберсигурност“ за ЕС и да бъде в състояние да разпознава признаци на кибератаки на достатъчно ранен етап и да позволява да се предприемат действия преди атаката да е нанесла щети. Допълнителните мерки ще включват специална подкрепа за малките и средните предприятия (МСП) в рамките на цифровите иновационни центрове , както и по-големи усилия за повишаване на квалификацията на работната сила, привличане и задържане на най-добрите специалисти в областта на киберсигурността и инвестиции в открити, конкурентоспособни и основани на високи постижения научни изследвания и иновации.

2. **Изграждане на оперативен капацитет за предотвратяване, възпиране и реагиране**

В рамките на поетапен и приобщаващ процес с участие на държавите членки Комисията подготвя ново съвместно кибернетично звено с цел да заздрави сътрудничеството между органите на ЕС и органите на държавите членки, които отговарят за предотвратяването, възпирането и реагирането на кибератаки по отношение на граждански общности, общности в областта на правоприлагането, дипломатически и кибернетични общности в областта на отбраната. Върховният представител представя предложения за засилване на инструментариума за кибердипломация на ЕС с цел да се предотвратява, възпира и реагира по ефективен начин спрямо злонамерени действия в киберпространството, по-специално такива, които засягат нашата критична инфраструктура, вериги на доставки, демократичните институции и процеси. ЕС ще се стреми още повече да засили сътрудничеството в областта на киберотбраната и да развие съвременни способности за киберотбрана, като се основава на работата на Европейската агенция по отбрана и насърчава държавите членки да използват пълноценно постоянното структурирано сътрудничество и Европейския фонд за отбрана.

3. **Постигане на напредък в създаването на световно и отворено киберпространство чрез засилено сътрудничество**

ЕС ще засили работата си със своите международни партньори с цел да укрепи основания на правила ред в световен мащаб, да насърчи сигурността и стабилността в киберпространството в международен план и да защити човешките права и основните свободи в интернет. ЕС ще предложи международни норми и стандарти, които отразяват тези основни ценности на ЕС, като си сътрудничи с международните си партньори в рамките на Организацията на обединените нации и други подходящи форуми. ЕС ще осигури освен това и допълнително усилване на своя инструментариум за кибердипломация и ще положи още повече усилия за изграждане на киберкапацитет с включване на трети страни чрез по-нататъшно развитие на Външната програма на ЕС за изграждане на киберкапацитет. Ще бъдат засилени диалозите по въпросите на кибернетичното пространство с трети държави, регионални и международни организации, както и с многостранната общност. ЕС ще създаде и мрежа на ЕС за кибердипломация по света с цел да популяризира своето виждане за киберпространството.

ЕС е ангажиран с подкрепата на новата стратегия за киберсигурност с безпрецедентно равнище на инвестиции в цифровия преход на ЕС през идните седем години чрез следващия дългосрочен бюджет на ЕС и по-специално чрез програмите „Цифрова Европа“ и „Хоризонт Европа“, както и чрез Плана за възстановяване на Европа . Държавите членки се насърчават да използват пълноценно Механизма за възстановяване и устойчивост на ЕС, за да се стимулира киберсигурността и да се съчетаят инвестициите на равнище ЕС. Целта е да се осигурят 4,5 милиарда евро комбинирани инвестиции от ЕС, държавите членки и промишлеността, по-специално в рамките на Центъра за компетентност в областта на киберсигурността, като се гарантира, че по-голяма част от тях достигат до МСП.

Комисията също така има за цел да укрепи промишления и технологичния капацитет на ЕС в областта на киберсигурността, включително чрез проекти, които се подкрепят съвместно от бюджета на ЕС и националните бюджети. ЕС разполага с уникалната възможност да обедини своите активи с цел да затвърди стратегическата си автономност и да засили водещата си роля в областта на киберсигурността по цялата цифрова верига на доставки (включително данните и облачното съхранение, технологиите за процесори от следващо поколение, ултрасигурната свързаност и мрежите 6G), в съответствие със своите ценности и приоритети.

Кибернетична и физическа устойчивост на мрежата, информационните системи и особено важните субекти

Съществуващите мерки на равнище ЕС, с които се цели защитата на ключови услуги и инфраструктури от кибернетични и от физически рискове трябва да бъдат актуализирани. С нарастването на цифровизацията и взаимната свързаност рисковете в областта на киберсигурността продължават да се увеличават. Справянето с физическите рискове също стана по-сложно след приемането на правилата на ЕС от 2008 г относно критичната инфраструктура, които понастоящем обхващат само секторите на енергетиката и транспорта. С преразглеждането се цели да се актуализират правилата в съответствие с логиката на стратегията на ЕС за Съюза на сигурност, да се преодолее погрешната дихотомия между „онлайн“ и „офлайн“ и се изостави едностранчивият подход.

За да се реагира по отношение на нарастващите заплахи, които се дължат на цифровизацията и взаимната свързаност, предложената директива относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (преработена Директива за МИС или „МИС 2“) ще обхване средни и големи субекти от различни сектори въз основа на нивото им на критичност за икономиката и обществото. С МИС 2 се засилват изискванията за сигурност, които се налагат на дружествата, работи се по сигурността на веригите на доставки и отношенията с

доставчиците, рационализират се задълженията за докладване, въвеждат се по-строги надзорни мерки за националните органи, както и по-строги изисквания за правоприлагане и се правят усилия за хармонизиране на режимите на санкции във всички държави членки. Предложението за МИС 2 ще помогне да се увеличи обменът на информация и сътрудничеството в областта на управлението на кризи в кибернетичното пространство на национално равнище и на равнище ЕС.

Предложената директива за устойчивост на особено важните субекти (УОВС) разширява както обхвата, така и задълбочеността на европейската Директива за критичната инфраструктура от 2008 г. Понастоящем са обхванати десет сектора: енергетика, транспорт, банково дело, инфраструктури на финансовите пазари, здравеопазване, снабдяване с питейна вода, цифрова инфраструктура, публична администрация и космическо пространство. В съответствие с предложената директива държавите членки ще приемат национални стратегии за гарантиране на устойчивостта на субектите от особено важно значение с цел да се гарантира устойчивостта им и редовно да се изготвят оценки на риска. С помощта на оценките ще се определи и една по-малка група от особено важни субекти, към които ще се прилагат изисквания за увеличаване на устойчивостта по отношение на рискове, различни от киберрисковете, включително оценки на риска на равнище предприятие, вземане на технически и организационни мерки и уведомяване за инциденти. От своя страна Комисията ще предоставя допълнителна подкрепа на държавите членки и особено важните субектите, например като изработва преглед на равнището на Съюза на трансграничните и многосекторните рискове, определя най-добрите практики, разработва методики, организира трансгранични дейности за обучение и учения за изпитване на устойчивостта на субектите от критично значение.

Гарантиране на сигурността на мрежите: 5G и мрежите от следващо поколение

В контекста на новата стратегия за киберсигурността държавите членки се приканват да завършат с подкрепата на Комисията и ENISA, Европейската агенция за киберсигурност, прилагането на инструментариума на ЕС за 5G — всеобхватен подход, основан на обективна оценка на риска, с който се работи по въпроса на сигурността на мрежите 5G и бъдещите поколения мрежи.

Според публикувания днесдоклад относно въздействието на Препоръката на Комисията относно киберсигурността на мрежите 5G и напредъка в прилагането на инструментариума на ЕС от смекчаващи мерки, и според доклада за напредъка от юли 2020 г., повечето държави членки вече са на път да приложат препоръчаните мерки. Сега те трябва се стремят да завършат прилагането на мерките до второто тримесечие на 2021 г. и да гарантират, че установените рискове са адекватно намалени по координиран начин, по-специално с цел да се сведат до минимум връзките с високорискови доставчици и да се избегне зависимостта от тези доставчици. Днес Комисията определя също така ключови цели и действия, насочени към продължаване на координираната работа на равнище ЕС.

Членовете на колегиума изразиха следните становища:

Маргрете **Вестегер**, изпълнителен заместник-председател с ресор „Европа, подготвена за цифровата ера", заяви: *„Европа е ангажирана с цифровата трансформация на нашето общество и икономика. Поради това ние трябва да я подкрепим с безпрецедентно равнище на инвестиции. Цифровата трансформация се ускорява, но може да има успех само ако хората и предприятията са сигурни, че свързаните продукти и услуги, на които те разчитат, са надеждни."*

Върховният представител Жозеп Борел заяви: *„Международната сигурност и стабилност зависят повече от всякога от едно глобално, отворено, стабилно и сигурно киберпространство, където се зачитат принципите на правовата държава, правата на човека, свободите и демокрацията. С представената днес стратегия ЕС се стреми да защитава своите правителства, граждани и предприятия от глобални кибернетични заплахи и да играе водеща роля в киберпространството, като гарантира, че всеки може да се възползва от предимствата на интернет и използването на технологиите."*

Заместник-председателят Маргаритис **Схинас**, отговарящ за утвърждаването на европейския начин на живот, заяви: *„Киберсигурността е централна част от Съюза на сигурност. Вече не съществува разграничаване между онлайн и офлайн заплахи. Цифровото и физическото измерение на живота понастоящем са взаимосвързани. Представените днес мерки показват, че ЕС е готов да използва всичките си ресурси и експертни познания, за да се подготвя за физически и кибернетични заплахи и да им дава адекватен отговор с еднаква решителност."*

Тиери **Бретон**, комисар по въпросите на вътрешния пазар, заяви: *„Киберзаплахите се развиват бързо, като стават все по-сложни и приспособими. За да сме сигурни, че гражданите и*

инфраструктурите са защитени, трябва да мислим с няколко стъпки напред; устойчивата и автономна европейския защита в областта на киберсигурността ще означава, че можем да използваме нашия експертен опит и знания, за да разпознаваме заплахите и да реагираме по-бързо спрямо тях, да ограничаваме потенциалните щети и да повишаваме устойчивостта си. Да инвестираме в киберсигурността означава да инвестираме в сигурното бъдеще на нашата онлайн среда и в стратегическата ни автономност."

Илва **Йохансон**, комисар по вътрешните работи, заяви: *„Нашите болници, системите за третиране на отпадъчни води или транспортна инфраструктура са само толкова сигурни, колкото е сигурно най-слабото им звено; смущения в една част на Съюза създават риск да бъде засегнато предоставянето на основни услуги на друго място. За да се осигури безпроблемното функциониране на вътрешния пазар и поминъкът на европейците, нашата ключова инфраструктура трябва да бъде устойчива спрямо рискове като природни бедствия, терористични атаки, инциденти и пандемии като тази, която преживяваме днес. Моето предложение относно критичната инфраструктура действа именно в тази посока.*"

Следващи стъпки

Европейската комисия и върховният представител са ангажирани да постигнат прилагането на новата стратегия за киберсигурност през следващите месеци. Те ще докладват редовно за постигнатия напредък, ще предоставят пълна информация на Европейския парламент, Съвета на Европейския съюз и заинтересованите страни и ще им осигуряват възможност да участват във всички съответни действия.

Сега Европейският парламент и Съветът трябва да разгледат и да приемат предложената директива МИС 2 и директивата относно устойчивостта на особено важните субекти. След като бъде постигнато споразумение по предложенията и впоследствие те бъдат приети, държавите членки ще трябва да ги транспонират до 18 месеца от датата на влизането им в сила.

Комисията периодично ще преразглежда Директивата МИС 2 и Директивата за устойчивостта на субектите от критично значение и ще докладва за тяхното функциониране.

Контекст

Киберсигурността е един от основните приоритети на Комисията и крайъгълен камък на цифровата и свързана Европа. Увеличаването на броя на кибератаките по време на кризата с коронавируса показа колко е важно да се защитят болниците, научноизследователските центрове и другите видове инфраструктура. В тази област са необходими решителни действия, за да се осигури съобразена с бъдещето защита на икономиката и обществото на ЕС.

В новата стратегия за киберсигурност се предлага киберсигурността да бъде интегрирана във всеки елемент от веригата на доставки и да се обединят дейностите и ресурсите на ЕС в четирите общности на киберсигурността – вътрешния пазар, правоприлагането, дипломацията и отбраната. Новата стратегия се създава на основата на виждането за Изграждане на цифровото бъдеще на Европа и на стратегията на ЕС за Съюз на сигурността, и се опира на редица законодателни актове, действия инициативи, които ЕС е приложил с цел да заздрави капацитета си в областта на киберсигурността и да гарантира по-устойчива в кибернетичен план Европа. Това включва стратегията за киберсигурността от 2013 г., която беше преразгледана през 2017 г., както и Европейската програма за сигурност за периода 2015–2020 г., В нея се признава нарастващата взаимосвързаност между вътрешната сигурност и сигурността спрямо външни заплахи, по-специално чрез общата външна политика и политиката на сигурност.

Първият приложим в целия ЕС закон за киберсигурността — Директивата за МИС , която влезе в сила през 2016 г., помогна да се постигне еднакво високо ниво на сигурност на мрежите и информационните системи навсякъде в ЕС. Като част от основната цел на политиката на Комисията да подготви Европа за цифровата ера през февруари тази година Комисията обяви преразглеждането на директивата за МИС. Актът на ЕС за киберсигурността, който е в сила от 2019 г., даде на Европа рамка за сертифициране на киберсигурността на продуктите, услугите и процесите и засили мандата на Агенцията на ЕС за киберсигурност (ENISA).

По отношение на киберсигурността на мрежите от пето поколение (5G) държавите членки с подкрепата на Комисията и ENISA създадоха инструментариум на ЕС за 5G – всеобхватен подход, основан на обективна оценка на риска, който беше приет през януари 2020 г. . Прегледът на препоръката на Комисията от март 2019 г. относно киберсигурността на мрежите от пето поколение (5G) установи, че повечето държави членки са постигнали напредък в прилагането на инструментариума.

Като се започне от стратегията на ЕС за киберсигурност от 2013 г., ЕС разработи последователна и цялостна международна политика в областта на киберсигурността. В сътрудничество с

партньорите си на двустранно, регионално и международно равнище ЕС насърчи установяването на глобално, отворено, стабилно и сигурно киберпространство, водено от основните ценности на ЕС и основано на принципите на правовата държава. ЕС помогна на трети държави да увеличат своята киберустойчивост и способност за справяне с киберпрестъпността и използва своя инструментариум от 2017 г. за кибердипломация с цел да даде допълнителен принос за международната сигурност и стабилност в киберпространството, в това число и като приложи за пръв път своя режим на санкции в киберпространството от 2019 г. и състави списък от 8 физически лица и 4 субекта и образувания. ЕС постигна значителен напредък и по отношение на сътрудничеството в областта на киберотбраната, включително по отношение на капацитета за киберотбрана, по-специално чрез политическата рамка на ЕС за киберотбрана, както и в контекста на постоянното структурирано сътрудничество (ПСС) и работата на Европейската агенция по отбрана.

Киберсигурността е приоритет, който е отразен и в следващия дългосрочен бюджет на ЕС (2021—2027г.). Съгласно Програмата „Цифрова Европа" ЕС ще подкрепя научните изследвания, иновациите и инфраструктурата в областта на киберсигурността, киберотбраната и промишлеността на ЕС в областта на киберсигурността. Освен това, в отговор на кризата с коронавируса, при която се отбеляза увеличаване на кибератаките по време на ограничителните мерки, в рамките на Плана за възстановяване на Европа се осигуряват допълнителни инвестиции в киберсигурността.

ЕС отдавна е признал необходимостта да се гарантира устойчивостта на инфраструктурите от критично значение, които предоставят услуги от съществено значение за безпроблемното функциониране на вътрешния пазар и за живота и поминъка на европейските граждани. Поради това през 2006 г. ЕС създаде Европейската програма за защита на критичната инфраструктура (ЕПЗКИ) и прие Директивата за европейската критична инфраструктура (ЕКИ) през март 2008 г., която се прилага в енергетиката и транспорта. През следващите години посочените мерки бяха допълнени от различни секторни и междусекторни мерки по конкретни аспекти като например устойчивостта на климата, гражданската защита и преките чуждестранни инвестиции.

За повече информация

Информационен документ за новата стратегия на ЕС за киберсигурност

Информационен документ предложението за директива относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (преразгледана директива за МИС)

Информационен документ относно киберсигурността: Външна дейност на ЕС

Въпроси и отговори: Нова стратегия на ЕС за киберсигурност и нови правила за повишаване на устойчивостта на физическите и цифровите особено важни субекти

Предложение за директива относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (преразгледана директива за МИС, или МИС 2)

Предложение за директива относно устойчивостта на особено важите субекти (вж. също Приложение 1 към предложението, както и оценката на въздействието и нейното резюме)

Европейски съюз на сигурност

Оценка на въздействието относно преразгледаната Директива за МИС („МИС 2")

Повече информация за киберсигурността

Повече информация за директивата за МИС

IP/20/2391

Лица за контакти с медиите:

Johannes BAHRKE (+32 2 295 86 15)
Adalbert JAHNZ (+ 32 2 295 31 56)
Nabila MASSRALI (+32 2 298 80 93)
Marietta GRAMMENOU (+32 2 298 35 83)
Laura BERARD (+32 2 295 57 21)
Xavier CIFRE QUATRESOLS (+32 2 297 35 82)

Въпроси на граждани: Europe Direct на телефон 00 800 67 89 10 11 или на електронния адрес на информационната служба

Related media

Illustration 2020/2