Комисията засилва реакцията на ЕС на кибератаки

Публикуван на: 20-09-2017
Източник: Портал Европа

Европейците възлагат голямо доверие на цифровите технологии. Те отварят нови възможности за свързване на гражданите, улесняват разпространението на информацията и изграждат гръбнака на европейската икономика. Те обаче също така доведоха до нови рискове, тъй като недържавни и държавни участници все по-често се опитват да крадат данни, да извършват измами и дори да дестабилизират правителства. През изминалата година са били извършвани повече от 4 000 кибератаки на ден посредством софтуер за изнудване и 80 % от европейските компании са станали жертва на поне една кибератака. Само за последните четири години икономическото въздействие от киберпрестъпността е нараснало петкратно.
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
Агенция на ЕС за киберсигурност: Като се използва опита на съществуващата Агенция на Европейския съюз за мрежова и информационна сигурност (ENISA), на новата агенция 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[1] 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. Това включва защитата на критичен хардуер и софтуер. За да се засили капацитетът на ЕС в областта на киберсигурността, Комисията и върховният представител 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 реагиратбързо**, оперативно и в унисон, когато започне мащабна кибератака. Предложената процедура е установена в препоръка, приета миналата седмица. 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, в началото на 2018 г. Комисията ще представи също така 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.