**МОТИВИ**

**КЪМ ЗАКОНА ЗА ИЗМЕНЕНИЕ И ДОПЪЛНЕНИЕ**

**НА НАКАЗАТЕЛНИЯ КОДЕКС**

Киберпрестъпността е обществено явление, което не признава граници, възползва се от постоянно разрастващата се глобализация, от новите технологии, от регионалните и националните кризи в страните – било то икономически, политически или военни. Ежедневно ставаме свидетели на мащабни и разнородни кибератаки, нанасящи огромни щети на компании и интернет потребители от цял свят, като същите са факт и в страната ни. Нещо повече, киберпрестъпността и употребата на Интернет пространството успешно и ефективно благоприятства и всяка една останала престъпна дейност на национално и транснационално ниво, която нанася огромни щети на бюджета.

В последното десетилетие е налице рязко и масово нахлуване на технологиите и интернет пространството в ежедневието на обществото ни като част от неговото развитие. С това във времето все повече се разширява и възможният обект на престъпления от подобен тип посегателства – засягат се както икономическите отношения (чл. 216, ал. 3-6, чл. 212а, чл. 246, ал. 3 , чл. 319а, чл. 319 б, чл. 319в НК), така и неприкосновеността на кореспонденцията ни (чл. 171 и чл. 319д НК), правата, защитаващи интелектуалната собственост, и други. Към днешната дата обект на компютърните престъпления могат да бъдат както държавата, така и бизнесът и гражданите.

Горепосоченото се потвърждава и от статистика на Главна дирекция „Борба с организираната престъпност“ към Министерството на вътрешните работи за постъпили сигнали от жертви на компютърни и компютърно свързани престъпления през последните 5 години, чиито показатели са следните:

|  |  |  |
| --- | --- | --- |
| **Година** | **Постъпили жалби и сигнали от жертви на киберпрестъпления** | **Взето отношение по**  **постъпилите жалби и сигнали имащи съставомерност по НК** |
| 2015 | 57 | 39 |
| 2016 | 757 | 543 |
| 2017 | 1308 | 971 |
| 2018 | 2384 | 1660 |
| 2019 | 2822 | 2049 |
| **Общо** | **7328** | **5262** |

**Таблица 1**

По данни от Годишния отчет за електронното управление за 2018-2019 година на Държавната агенция „Електронно управление“ в периода август 2018 г.-юли 2019 г. Националният екип за реагиране при инциденти с компютърната сигурност към Държавната агенция „Електронно управление“ констатира непрекъснато усложняване на обстановката в киберсигурността на страната.

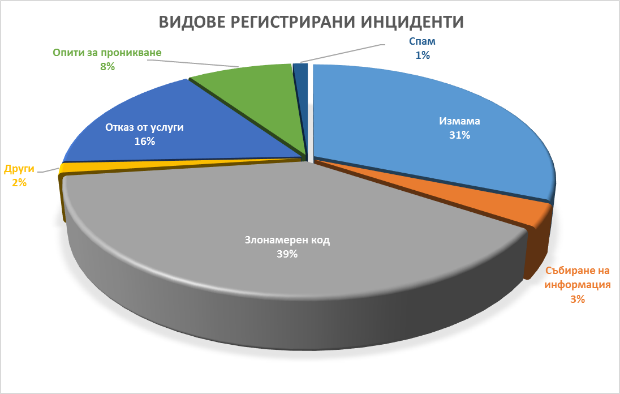
В таблицата по-долу е показана статистика за отчетния период, свързана с регистрирани инциденти в централните и териториалните администрации с мрежовата и информационната сигурност с висок и среден приоритет.

|  |  |  |
| --- | --- | --- |
| **№** | **Тип на инцидента** | **Брой засегнати администрации** |
| 1 | DDoS (разпределен отказ от услуга) | 13 |
| 2 | Ransomware (криптиращ вирус) | 4 |
| 3 | Instrusion Attempts (общо проникване) | 1 |
| 4 | Unauthorised Access to information (неоторизаран достъп до информация) | 9 |
| 5 | Кражба на лични данни | 1 |
| 6 | Уязвимост | 2 |
| 7 | Phishing (измамнически сайт) | 3 |
| 8 | SQL injection | 2 |

**Таблица 2**

По данни от статистиката, която се води от Екипа за нарушения в и от българското Интернет пространство, са регистрирани 2 851 сигнала, което е с 34% увеличение спрямо предходния период. От тях като инциденти, съгласно таксономията на Европейската агенция за киберсигурност – ENISA, са регистрирани 2 030, което е увеличение с 33%. Наблюдава се рязко увеличаване на броя засегнати IP адреси в българското адресно пространство – над 6.5 пъти.

Данните от статистиката също показват, че рязко нараства относителният дял на инцидентите със значително увреждащо въздействие в мрежовата и информационната сигурност с висока степен на опасност. Най-голям е процентът на регистрираните инциденти, дължащи са на злонамерен код (malware), следвани от инцидентите, дължащи се на измама (phishing).

*Фиг. 1 Обем на базите данни*

Хакерски групи продължават да се насочват към субекти в държавите членки на ЕС, в т.ч. и България, с цел придобиване на чувствителна информация. Най-значимите атаки на тези групи са насочени към мрежови устройства като рутери, комутатори, защитни стени, мрежово базирани системи за откриване на прониквания (Intrusion Detection System), разположени в мрежите предимно на правителствени и частни организации, ръководители на обекти от критичната инфраструктура и доставчици на достъп до интернет (ISP), които поддържат тези сектори.

Националният екип за реагиране при инциденти с компютърната сигурност ежемесечно в изпълнение на проактивните си действия изпраща бюлетин до служителите в публичната администрация, отговарящи за мрежовата и информационната сигурност. Бюлетинът съдържа статистика на инцидентите за предходния месец, информация и препоръки за добри практики.

В допълнение на това в годишния си доклад за 2019 година Центърът по киберсигурност към Европол също отчита, че киберпрестъпленията стават все по-дръзки, а фокусът им се измества към по-големи и по-печеливши цели. В тази връзка Центъра по киберсигурност препоръчва, една от мерките за справяне на държавите членки да бъде прилагане на закон, който трябва да бъде еднакво дързък, за да отговори на предизвикателството и в тази връзка законодателството на държавите членки да еволюира съобразно постоянно променящите се и развиващи се технологии.

В доклада се посочва също така тревожна статистика по отношение на т.нар. компютърен саботаж в частния сектор, а именно компютърните престъпления, при които не само неправомерно се достъпва дадена информационна система, но и данните в нея се увреждат или унищожават с цел затрудняване работата на съответното юридическо лице. Това води до нарастващ страх у частния сектор. Статистиката през първите 6 месеца на 2019 година показва, че кибератаките, предназначени да причиняват щети, са се удвоили, като 50% от атакуваните фирми са били в производствения сектор. Това принуждава частният сектор да прави вложения в защитени резервни копия на данните, тъй като иначе биха загубили трайно своите данни.

Също така на 14 октомври 2019 г. в Министерството на правосъдието постъпи официално уведомително писмо на Европейската комисия (ОУП) № С (2019) 6272 по процедура за нарушение № 2019/2240 относно неизпълнение на задълженията на Република България във връзка с чл. 9, пар. 4, буква „б“ и буква „в“ от Директива 2013/40/ЕС относно атаките срещу информационните системи. Според констатациите на Европейската комисия при транспонирането на Директива 2013/40/ЕС България не се е съобразила с изискуемия максимален праг на наказанието лишаване от свобода, предвиден в случаите, посочени в чл. 9, пар. 4 от Директивата, който следва да бъде не по-малък от пет години. Този праг се предвижда, когато деянията по чл. 4 и 5 от Директивата са причинили сериозни вреди или са извършени срещу информационна система, която е част от критична инфраструктура.

Особено важно за нормалното функциониране на държавата е осигуряването на безпроблемната работа както на държавния апарат, така и на обектите от стратегическо значение в различните структуроопределящи сектори, като земеделието, транспорта, енергетиката, здравеопазването и други. Това е т.нар. критична инфраструктура. Нарушаването на нормалното й функциониране може да доведе освен до сериозни финансови загуби, до заплаха за националната сигурност на страната, а също и до нарушаване на нормалното снабдяване на обществото с жизнено важни услуги и/или продукти. През 2019 година в европейски план се наблюдава разширяване на обхвата на представляващите критична инфраструктура обекти от разследващите органи в европейските държави, като дължащо се както на повишената бдителност на националните компетентни органи, така и на увеличаващия се брой кибер атаки.

Същевременно по линия противодействие този вид престъпления, извършени в и чрез дигитална среда, са налице трудности при документиране на престъпната дейност и установяване на извършителя, произтичащи от настоящата законодателна уредба и по-конкретно от Закона за електронните съобщения (ЗЕС) и Наказателния кодекс (НК). Съгласно чл. 251б, ал. 2 от ЗЕС се регламентира, че компютърно-информационни данни могат да се изискват по съответния ред, само когато са свързани с извършено тежко умишлено престъпление – тоест предвидено е наказание над 5 години лишаване от свобода.

В същото време това е и единственият начин за събиране на дигитални следи, от които може да се достигне до извършителя на престъплението. Подобна е правната уредба и на деянията по чл. 319г от НК, касаещи въвеждането на компютърен вирус в информационна система или компютърна мрежа, както и въвеждането на друга компютърна програма, която е предназначена за нарушаване на дейността на информационна система или компютърна мрежа или за узнаване, заличаване, изтриване, изменение или копиране на компютърни данни без разрешение, когато такова се изисква. Противоправни деяния, изразяващи се в неправомерно осъществен достъп до информационна система или части от нея, при които не са настъпили тежки последици, както и при достъп до или промяна на компютърни данни в информационна система, когато това не е свързано е дейността на организирана престъпна група или достъпът не касае критична инфраструктура, също на практика не могат да бъдат ефективно разследвани и пресичани.

Престъпленията срещу интелектуалната собственост, авторското право и сродните му права (Глава трета, раздел VII от НК) са деяния с висока степен на обществена опасност, не само предвид правата и интересите на авторите, които засягат, а и с нанасянето на финансови загуби в особено големи размери, което се отразява на приходите в държавния бюджет. Тяхното разследване също е невъзможно да бъде извършено без изискване на т.нар. „трафични данни“.

Същевременно децата, като едни от най-малките и най-активни потребители на интернет пространството са ежедневно изложени на порнографско съдържание, което още от ранна възраст провокира деструктивно действие върху оформянето на личността им. Нещо повече, малолетни и непълнолетни ежедневно стават жертви на сексуални набези от страна на лица, имащи такъв тип сексуално поведение. В тази връзка са необходими спешни промени и на съставите на престъпления в Глава втора, раздел VIII от НК -„Разврат“.

От изложеното по-горе става ясно, че освен наличието на усложнена кибер обстановка както в Република България, така и в Европейския съюз, е налице необходимост и от осигуряване на възможност на правоохранителните органи пълноценно да могат да извършват разследвания на компютърните престъпления, извършвани на територията на страната.

Така формулирана, нормата на чл. 251б, ал 2 от ЗЕС не позволява придобиването й по единствения възможен начин на значимата информация за разкриването на престъпления срещу почти всички състави на визираните по-горе престъпления:

- за същинските компютърни престъпления от Глава девета „а“ от НК;

- за компютърно свързаните престъпления в Глава втора, раздел VIII от НК - онлайн детска сексуална експлоатация и Глава трета, раздел VII от НК – интелектуална, индустриална собственост и авторско право.

Съставите на горепосочените престъпления предвиждат наказания „лишаване от свобода“ по-малко от 5 години или до 5 години. От друга страна, за ефективното им разследване и наказателно преследване е необходимо да бъде получена информация по чл. 251б от ЗЕС (трафични данни). Съгласно ал. 2 на същия такива данни се съхраняват за нуждите на националната сигурност и за предотвратяване, разкриване и разследване на тежки престъпления. В този смисъл е и решение на Конституционния съд № 2 от 12 март 2015 г. по конституционно дело № 8 от 2014 г. Със същото съдът обявява за противоконституционни актуалните към 2014 г. текстове на ЗЕС, като намира, че същите не удовлетворяват установените европейски стандарти за гарантиране на конституционно закрепените основни права на гражданите. Решението на Конституционния съд е в пряка връзка с Решение на Съда на ЕС от 8.04.2014 г., разширен състав, по съединени дела С-293/12 и С-594/12, (по-известно като Digital rights Ireland) с което транспонираната в ЗЕС Директива 2006/24/ЕО е обявена за невалидна поради несъответствието й с разпоредбите на чл. 7, чл. 8 и чл. 52, § 1 от Хартата на основните права на Европейския съюз. Съдебната практика на Съда на ЕС относно съхранението на данни е доразвито с Решение на Съда от 21.12.2016 г. по съединени дела C 203/15 и C 698/15 (известно и като Tele 2 & Watson). В същото Съда на ЕС потвърждава, че събирането на трафични данни е мярка, чийто характер предпоставя сериозно ограничаване на правото на личен и семеен живот и на правото на защита на личните данни (защитени в чл. 7 и чл. 8 от Хартата на основните права на ЕС), поради което достъп до трафични данни е възможен само за целите на превенция, разследване и наказателно преследване на тежки престъпления. Така практиката на Съда на ЕС прави невъзможно използването на трафични данни при извършени престъпления, които не са тежки по смисъла на националното законодателство на всяка държава членка.

От описаните по-горе проблеми става ясно, че се налага актуализиране на действащата нормативна уредба на компютърните и компютърно свързаните престъпления в Наказателния кодекс, във връзка с което и с оглед осигуряване на по-адекватна защита на държавата, бизнеса и гражданите от неправомерни деяния, засягащи техните основни права, предлагаме в Глава втора, раздел VIII, Глава трета, раздел VII и Глава девета „а“ от НК увеличаване на размера на наказанията в НК и включване квалифицирани състави на престъпления за компютърни и компютърно свързани престъпления с оглед постигане на съответствие между обществената опасност на тези престъпления и предвидените от закона наказания.

В последните години се наблюдава тенденция на дигитализиране и автоматизиране на все повече услуги и процеси, които са свързани както със стопанския живот, така и с ежедневните дейности на гражданите. Съвременните технологии позволяват сключване на сделки, банкови трансфери, съхранение на и достъп до лични данни и друга чувствителна информация онлайн. Блокчейн като иновативна технология за верифициране навлиза във все по-широк кръг обществени отношения. На практика няма дейност, която да се осъществява без електронен обмен на дигитална информация. Компютрите се превръщат в средство за извършване на повечето престъпления, инкриминирани в НК. Увеличаването на възможностите на компютърните технологии води и до увеличаване на опасностите и възможностите за засягане на правата на гражданите. По тази причина все по-широк кръг обществени отношения са засягани от компютърни престъпления или от престъпления, извършени чрез използване на компютърни мрежи или системи. От друга страна се наблюдава тенденция към увеличаване на тежестта на засягане на обществените отношения от компютърни и компютърно свързани престъпления. Изграждането на автоматизирани информационни бази данни прави възможно засягането на много широк кръг лица, създавайки условия за последващо извършване на множество други престъпления, засягащи правата на широк кръг лица.