Стопански факултет

Социално-икономически анализи

Книга 2/2024 (25)

DOI:10.54664/APKX2659

Димитър Петков*

УПРАВЛЕНИЕ НА СИГУРНОСТТА В БЪЛГАРИЯ – НОВ МОДЕЛ НА ДОБРИТЕ ПРАКТИКИ

Dimitar Petkov

SECURITY MANAGEMENT IN BULGARIA – A NEW MODEL OF GOOD PRACTIC

Abstract: Modern information and communication technologies make life extremely fast and significantly easier, but at the same time they raise the shadow of the threat of the deadliest type of crime - cybercrime. Without computers, however, entire businesses and organizations in the public and private sectors would virtually cease to function. This proliferation of cheap, powerful, easy-to-use machines enables more and more people to use them and, more importantly, rely on them as part of their normal lifestyle. As companies, public organizations and individuals continue to rely on them more and more, so do criminals. Reducing cybercrime depends on properly analyzing the behaviour of offenders and understanding their impact on different levels of society.

Key words: energy security, energy policies, energy security threats, problems and solutions

Въведение

Съвременните информационни и комуникационни технологии правят живота изключително бърз и значително по-лесен, но едновременно с това хвърлят сянката на заплахата от един от най-смъртоносните видове престъпност – киберпрестъпността. Без компютри обаче цели предприятия и организации от публичния и частния сектор на практика биха престанали да функционират. Това разпространение на евтини, мощни, лесни за употреба машини дава възможност на все повече и повече хора да ги използват и, което е по-важно, да разчитат на тях като част от нормалния си начин на живот. Тъй като компаниите, публичните организации и отделните лица продължават да разчитат на тях все повече и повече, същото се отнася и за престъпниците. Ограничаването на киберпрестъпленията зависи от правилния анализ на поведението на нарушителите и разбирането на тяхното въздействие върху различни нива на обществото.

Видове компютърни престъпления. Престъпления, свързани с данни

Киберпрестъпник наблюдава потоци от данни към или от цел, за да събере информация. Тази атака може да бъде предприета, за да се събере информация в подкрепа на последващо напа-

* **Димитър Петков** – докторант, Докторант в катедра „Управление“ на УНСС, e-mail: stefipetkovapanova @abv.bg

дение или събраните данни може да са крайната цел на атаката. Тази атака обикновено включва подслушване на мрежов трафик, но може да включва наблюдение на други видове потоци от данни, като например радио. В повечето разновидности на тази атака нападателят е пасивен и просто наблюдава редовната комуникация, но в някои варианти той може да се опита да инициира установяването на поток от данни или да повлияе на естеството на предаваните данни. Въпреки това, във всички варианти на тази атака и разграничавайки я от другите методи за събиране на данни, атакуващият не е предвиденият получател на потока от данни.

За разлика от някои други атаки с изтичане на данни, нападателят наблюдава изрични канали за данни (напр. мрежов трафик) и чете съдържанието. Това се различава от престъпленията, които събират повече качествена информация, като обем на комуникация, която не е изрично комуникирана чрез поток от данни[1].

Модифициране на данни

Поверителността на комуникациите е от съществено значение, за да се гарантира, че данните не могат да бъдат модифицирани или преглеждани по време на пренос. Разпределените среди носят със себе си възможността злонамерена трета страна да извърши компютърно престъпление чрез подправяне на данни, докато се движат между сайтове[2].

При атака за модифициране на данни неупълномощена страна в мрежата прихваща данни по време на транзит и променя части от тях, преди да ги препредаде. Пример за това е промяната на сумата в долари на банкова транзакция от $100 на $10 000. При повторна атака, цял набор от валидни данни се намесва многократно в мрежата. Пример би бил да се повтори хиляда пъти валидна транзакция за банков превод на стойност $100.

Терминът **кражба на данни** е използван за описание на случаите, когато информацията е незаконно копирана или взета от бизнес или друго лице. Обикновено тази информация е потребителска – пароли, осигурителни номера, информация за банкова карта, друга лична информация или друга поверителна корпоративна информация. Тъй като тази информация е получена незаконно, когато лицето, което я е откраднало, бъде задържано, е вероятно то да бъде преследвано с цялата строгост на закона[3].

Мрежова престъпност. Мрежови смущения

Представляват намеса във функционирането на компютърна мрежа чрез въвеждане, предаване, повреждане, изтриване, влошаване, промяна или потискане на мрежови данни.

– **Мрежов саботаж**

Освен целенасочени злонамерени действия, тук се нареждат и някои прояви на некомпетентност. Често не може да бъде установено дали мрежовите проблеми са резултат от едното или другото[4].

Престъпления, свързани с достъпа. Неоторизиран достъп

Неоторизиран достъп възниква, когато лица получат достъп до мрежи, системи, приложения, данни или устройства на организация без разрешение. Това обикновено включва пробив в сигурността на мрежата, който може да компрометира целостта ѝ или да доведе до загуба на данни. Често срещаните причини включват слаби пароли, фишинг атаки и неадекватна физическа сигурност. За предотвратяване на неупълномощен достъп е от съществено значение да се приложат

[1] CAPEC (2010), CAPEC-117: Data Interception Attacks, http://capec.mitre.org/data/definitions/117.html последно посетен на 30.04.2024

[2] Oracle (2003), Security Overviews, http://docs.oracle.com/cd/B13789_01/network.101/ b10777/overview.htm последно посетен на 30.04.2024

[3] Computer Hope (2012), Data Theft, http://www.computerhope.com/jargon/d/datathef.htm последно посетен на 30.04.2024

[4] DSL Reports (2011), Network Sabotage, http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to- последно посетен на 30.04.2024

силни мерки за сигурност, като стабилни политики за пароли, многофакторно удостоверяване, редовни софтуерни актуализации, обучение на служителите за информираност относно сигурността и ефективни практики за физическа сигурност[5].

– **Разпространение на вируси**

Вирусът представлява зловреден софтуер, който се свързва с друг софтуер – червеи, троянски кон ,“бомба със закъснител”, “логическа бомба” са примери за злонамерен софтуер, който унищожава системата на жертвата[6].

Свързани престъпления . **Подпомагане и съучастие**

Има три елемента, характерни за повечето обвинения за помагачество и съучастие. На първо място, друго лице е извършило престъплението – от тази гледна точка съучастникът обикновено се определя като лице, което подпомага престъпление, извършено от друг или други. В повечето случаи лице, обвинено в помагачество и съучастие, е знаело за престъплението преди или след неговото извършване, и е оказвало някаква форма на помощ на тези, които извършват престъплението. В юридическата теория такъв помагач е известен като „съучастник преди факта.“ Той или тя може да помогне чрез съвети, действия или парична подкрепа. Лице, което не е наясно с престъплението, преди то да се извърши, но което помага след престъплението, се нарича „съучастник след факта“[7].

– **Свързани с компютър фалшификации и измами**

Компютърните фалшификации и свързаните с компютър измами са такива, за чието извършване са използвани възможностите на съвременните информационни и комуникационни технологии.

– **Престъпления, свързани със съдържание**

Кибер секс, непоискани търговски съобщения, кибер клевета и кибер заплахи са включени в списъка на престъпленията, свързани със съдържание. Общата цена, която жертвите трябва да платят срещу тези атаки, възлиза на милиони долари годишно.

– **Международен опит в борбата с киберпрестъпленията**

Много е важно да се разбере глобалният характер на проблема с киберпрестъпността. Кибератаките вече парализират работата не само на частни структури, но и на държавни органи и няма държава в света, която да е защитена от подобни атаки. Не само хакерите или техните групи, но и отделни страни, терористични и престъпни групи се считат за вероятни източници на киберзаплахи. При разработването на инструменти и методи за борба с киберпрестъпността трябва да се има предвид латентността на този вид престъпност.

Според експерти, латентността на компютърните престъпления в САЩ достига 80%, във Великобритания – 85%, в Германия – 75%[8]. Според международната услуга за киберсигурност Symantec Security всяка година в света се регистрират около 556 милиона киберпрестъпления със загуби от над 100 милиарда долара[9]. Киберпрестъпността може да наруши интересите както на държавата, така и на индивида.

Несъмнено особеностите на функциониране на информационните системи, особено на Интернет, изискват съвместните усилия на различни участници, както публични, така и частни, да бъдат насочени към решаване на проблемите на киберсигурността[10]. Само държавата обаче може и е в състояние да се бори ефективно с пълномащабната киберпрестъпност, да създаде условия за

---

[5] **NordVPN** (2023) https://nordvpn.com/blog/unauthorized-access/ последно посетен на 30.04.2024

[6] **Virus Glossary** (2006) Virus Dissemination, http://www.virtualpune.com/citizencentre/html/cyber_crime_glossary.shtml последно посетен на 30.04.2024

[7] **Legal Info** (2009), Crime Overview aiding and abetting or Accessory, http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory. html последно посетен на 30.04.2024

[8] **Statista.** 2020. The level of penetration of the Internet in the world. https://www.statista.com/statistics/269329/penetration-rate-of-the-internetby-region/ последно посетен на 30.04.2024

[9] **Belsky, Y.** (2014). On the definition of cybercrime Legal Bulletin. Vol. 6, pp. 414–418.

[10] **Rogovets, V.** (2015) Information wars in the modern world: causes, mechanisms, consequences Personnel. No. 5, pp. 10–17.

тези, които са най-уязвими на такива атаки, да изгради по-надеждна система за информационна сигурност.

В момента водещите страни в света активно разширяват и създават звена във въоръжените сили и разузнавателните служби, които трябва да осигурят развитието на нападателни способности в киберпространството. Например в Съединените щати, заедно с Националния център за киберсигурност, в рамките на въоръжените сили е създадено Съвместното киберкомандване, което трябва да координира усилията на всички структури на Пентагона в хода на военните действия, да предоставя подходяща подкрепа към цивилни федерални агенции и взаимодейства с подобни агенции в други страни (Министерство на отбраната на САЩ, 2009 г.).

В същото време тези организации са частично контролирани агенции, като върховната контролна структура е Съветът за национална сигурност със специална комисия, чиито отговорности включват прилагането на информационна стратегия[11], включително борбата с киберпрестъпността.

В Обединеното кралство се изпълняват програми за кибероръжия, които ще позволят на правителството да устои на нарастващите заплахи от киберпространството[12].

В Австралия е създадена група за координация на сигурността на електронната поща (ESCG). Основната задача на тази група е да създаде сигурно и надеждно електронно оперативно пространство както за публичния, така и за частния сектор[13].

Дейностите за борба с киберпрестъпността се извършват не само от отделни държави, но и от техните блокове, включително НАТО. Така важността на този проблем е отразена във всички ръководни документи на блока, приети през последните години. За първи път стратегическата концепция на НАТО включва киберпространството като нова област на военния съюз. С други думи, в борбата с трансграничните престъпления, които включват значителна част от киберпрестъпността, специална роля се дава на държавите и само с добре координирани правоприлагащи органи на различни страни е възможно да се намали броят на престъпленията, извършени в тази област. Международното сътрудничество се осъществява в няколко области и включва на първо място създаването на регламенти и разработването на общи препоръки, както и въвеждането на ефективни модели на организационно взаимодействие между държавите. Трябва да се има предвид, че традиционните механизми на международно сътрудничество, включително молби, взаимопомощ и други подобни инструменти, използвани през XIX век, са неподходящи в епоха, когато престъпленията могат да се извършват от всяка точка на света със скоростта на светлината[14].

Правното регулиране на борбата с киберпрестъпността е в основата на цялата система за борба с киберпрестъпността. Сложността на изготвянето на международни актове като цяло в разглежданата ситуация се усложнява допълнително от факта, че съществуващите закони са трудни за прилагане, когато става въпрос за нелокализирани атаки в планетарен мащаб, доказателствата за които са разпръснати и виртуални[15].

Международната общност на различни равнища е разработила редица актове, свързани с борбата с киберпрестъпността, като регионалните актове играят специална роля, тъй като глобалните документи в момента са трудни за създаване. В същото време е важно да се отбележат опитите на държавите да разширят нормите на глобалните международни договори за борба с киберпрестъпността или да сключат нови договори. Например, тъй като организираните престъпни

[11] **Djerf-Pierre, M.** (2018) Squaring the circle: public service and commercial news on Swedish television Journalism Studies. Vol.1, No. 2, 239–260.

[12] **Kessel, J.; Mozur, P.** (2016) How China Is Changing Your Internet https://www.worldpressphoto.org/collection/storytelling/2017/29057/2017-how-china-is-changing-your-internet последно посетен на 30.04.2024..

[13] **Sanders, K., Canel Crespo, M. J., Holtzs-Bacha, Ch.** (2017) Communicating governments: a three-country comparison of how governments communicate with citizens The International Journal of Press/Politics. Vol. 16, No. 4, pp. 82–96.

[14] **Wang, SY K** (2021) Collaboration between law enforcement agencies in combating cybercrime: implications of a Taiwanese case study about ATM hacking International journal of offender therapy and comparative criminology. Vol. 65, No. 4, pp. 390–408.

[15] **Pozhuyev, V** (2016) Formation of the state information policy in the conditions of globalization Humanitarian bulletin of the Zaporozhye state engineering academy. Vol. 43, pp. 4–12.

групи могат да действат заедно с отделни лица в киберпространството, е възможно да се прилагат към тях международни договори, насочени към борба с организираната престъпност, по-специално Конвенцията на ООН срещу транснационалната организирана престъпност от 15 ноември 2000 г, наред с концепцията на Конвенцията на ООН за международна информационна сигурност както е разработен[16]. Основната част на документа се състои от пет раздела, чието съдържание е в единна композиционна цялост.

Важно е, че в чл. 4 от Конвенцията основните заплахи за международния мир и сигурност в информационното пространство са идентифицирани, единадесет от които са основни и четири допълнителни. Сред основните са посочени например използването на информационни технологии и инструменти за враждебни действия и прояви на агресия; целенасочено деструктивно въздействие в информационното пространство върху критични структури на друга държава, трансгранично разпространение на информация, която противоречи на принципите и нормите на международното право, както и на националните закони на държавите. В документа обаче не се споменават такива реални заплахи за международната сигурност като извършването на киберпрестъпления, разпространението на наркотици и психотропни вещества, техните аналози, както и порнографията, включително детската порнография. Чл. 5 от Конвенцията е посветен на основните принципи на международната информационна сигурност.

Анализът на посочените по-горе принципи позволява да се заключи, че те могат да бъдат разделени на четири групи:

- принципи на участие на държавата в системата на международната информационна сигурност като член на международната общност;
- принципи, които позволяват на държавата да запази своя суверенитет в процеса на международно сътрудничество в борбата с киберпрестъпността;
- принципи за осигуряване на свободен обмен на информация между страните;
- принципи за установяване характера на взаимодействието на държавата и частните субекти в разглежданите отношения.

В същото време трябва отново да се отбележи, че концепцията на Конвенцията не предписва подробно принципите на международното сътрудничество в борбата с киберпрестъпността, с изключение на целенасочената борба с тероризма.

Включването на раздел 5 „Международно сътрудничество в областта на международната информационна сигурност“ в концепцията на Конвенцията трябва да се признае за положително, но мерките за международно сътрудничество в тази област са недостатъчни за ефективното функциониране на системата за международна икономическа сигурност. Такива мерки включват само обмен на национални концепции за сигурност в информационното пространство, оперативен обмен на информация за кризисни събития и заплахи в информационното пространство и мерки, предприети за тяхното разрешаване и неутрализиране, консултации относно дейностите в информационното пространство. Тези форми обаче не се приемат с оглед отчитане необходимостта от оперативно сътрудничество на правоприлагащите органи по широк кръг въпроси. По този начин разпоредбите на концепцията на Конвенцията на ООН за международна информационна сигурност са доста компромисно и насочени предимно към предотвратяване на информационни войни, тероризъм.

Европейски програми за борба с киберпрестъпността

Трябва да се отбележи, че повечето от специализираните актове за борба с киберпрестъпността са такива на Европейския съюз, който разполага с една от най-развитите системи за информационна сигурност в света. През 2001 г. Европейската комисия представя специално съобщение, съдържащо предложения от правно и организационно естество за борба с киберпрестъпността

[16] **Butunbaev, T.** (2020) Features Of International Legal Cooperation Combating Cyber Crime International Journal of Advanced Research (IJAR). Vol. 8, No. pp. 05, 100–107 http://dx.doi.org/10.21474/IJAR01/10911 последно посетен на 30.04.2024

в ЕС. Програмите на Интерпол са изградени около подготовката на операциите за борба с нови компютърни заплахи. Те са насочени към:

- улесняване на обмена на информация между държавите членки в рамките на регионални работни групи и конференции;
- подготовка на курсове за обучение за създаване и поддържане на професионални стандарти;
- координиране и улесняване на международни операции;
- създаване на глобален списък с контакти за разследване на киберпрестъпления;
- подпомагане на държавите-членки в случай на кибератаки или киберпрестъпления в разследвания чрез бази данни;
- развитие на стратегическо партньорство с други международни организации и организации от частния сектор;
- откриване на нови заплахи и предаване на разузнавателна информация на държави-членки;
- осигуряване функционирането на защитен уеб портал за достъп до оперативна информация и документи.

Заключение

Бъдещето на интернет все още е за престъпници и нормални потребители. Страховете от кибер-апокалипсис все още изобилстват, докато потенциалният размер на щетите, които могат да бъдат причинени от широкомащабни измами, е почти неограничен. Тези тревоги трябва да бъдат смекчени рационално със знанието, че проблемите се решават, макар и може би не достатъчно бързо. Полезността на Интернет се е доказала по многобройни и безброй начини, които се надяваме да са достатъчни, за да гарантират, че няма да се превърне в пустош на престъпна дейност и бастион за злонамерените. Правителството все още играе важна роля, но по-голямата част от превенцията трябва да се извършва от търговски субекти, произвеждащи софтуер, и тези, които имат способността да спират измамите. Разчитането на програми за обучение на потребителите ще засегне само процент от възможните жертви. Другите трябва да бъдат автоматично защитени чрез мерки, които не натоварват и изискват значително участие. Сигурността трябва да е лесна и ефективна, ако върши работа. Дали киберпрестъпността все още е уместен проблем след десет години е неизвестен в известен смисъл, но ако интернет ще продължи да се разраства, той трябва да бъде решен, така че реалностите на киберпрестъпността да бъдат пропорционални на престъпленията в реалния свят, ако не и по-добри.

ЛИТЕРАТУРА

Belsky, Y. On the definition of cybercrime Legal Bulletin. Vol. 6, 2014, pp. 414–418. // Butunbaev, T. (2020) Features Of International Legal Cooperation Combating Cyber Crime International Journal of Advanced Research (IJAR). Vol. 8, No. pp. 05, 100–107 http://dx.doi.org/10.21474/IJAR01/10911 последно посетен на 30.04.2024

CAPEC CAPEC-117: Data Interception Attacks, 2010. http://capec.mitre.org/data/definitions/117.html последно посетен на 30.04.2024.

Computer Hope Data Theft, 2012. http://www.computerhope.com/jargon/d/datathef.htm последно посетен на 30.04.2024.

Council of Europe European Convention on Cybercrime, 2001. https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf последно посетен на 30.04.2024

Djerf-Pierre, M. Squaring the circle: public service and commercial news on Swedish television Journalism Studies. Vol.1, No. 2, 2018, 239–260.

Dremliuga, R. Dremliuga, O. Kuznetsov, P. Combating the threats of cybercrimes in Russia evolution of the cybercrime laws and social concern Communist and post-communist studies. Vol. 53, No. 3, pp. 2020, 123–136.

DSL Reports Network Sabotage, 2011. http://www.dslreports.com/forum/r26182468-Network-Sabotage-or-incompetent-managers-trying-to- последно посетен на 30.04.2024.

EUROPOL Internet Organised Crime Threat Assessment 2018. https://www.europol.europa.eu/activities-services/main-reports/internet-organisedcrime-threat-assessment-iocta-2018 последно посетен на 30.04.2024

Kessel, J., Mozur, P. How China Is Changing Your Internet 2016. https://www.worldpressphoto.org/collection/storytelling/2017/29057/2017-how-china-is-changing-your-internet последно посетен на 30.04.2024

Legal Info Crime Overview aiding and abetting or Accessory, 2009. http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory. html последно посетен на 30.04.2024

NordVPN 2023 https://nordvpn.com/blog/unauthorized-access/ последно посетен на 30.04.2024

Oracle Security Overviews, 2003. http://docs.oracle.com/cd/B13789_01/network.101/ b10777/overview. htm последно посетен на 30.04.2024

Pozhuyev, V. Formation of the state information policy in the conditions of globalization Humanitarian bulletin of the Zaporozhye state engineering academy. Vol. 43, 2016, pp. 4–12

Rogovets, V. Information wars in the modern world: causes, mechanisms, consequences Personnel. No. 5, 2015, pp. 10–17.

Sanders, K., Canel Crespo, M J., Holtzs-Bacha, Ch. Communicating governments: a three-country comparison of how governments communicate with citizens The International Journal of Press/Politics. Vol. 16, No. 4, 2017, pp. 82–96

Statista. The level of penetration of the Internet in the world, 2020. https://www.statista.com/statistics/269329/penetration-rate-of-the-internetby-region/ последно посетен на 30.04.2024

UN European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI), 2021. https://www.unodc.org/unodc/en/commissions/CCPCJ/PNI/institutes-HEUNI.html последно посетен на 30.04.2024

US Department of Defense Report on Strategic Communication, 2009. https://www.hsdl.org/?view&did=716396 последно посетен на 30.04.2024

Virus Glossary Virus Dissemination, 2006. http://www.virtualpune.com/citizencentre/html/cyber_crime_glossary.shtml последно посетен на 30.04.2024

Wang, SY K Collaboration between law enforcement agencies in combating cybercrime: implications of a Taiwanese case study about ATM hacking International journal of offender therapy and comparative criminology. Vol. 65, No. 4, 2021, pp. 390–408.