КИБЕР СИГУРНОСТТА В УСЛОВИЯТА НА ИНТЕГРИРАНА СИГУРНОСТ

Ю. Каракънева

Съвременната среда за сигурност се отличава с нови, доскоро неподозирани измерения. Класическото противопоставяне на политики и военна мощ отстъпва място на новите технологии и новите сблъсъци.

Основните характеристики на съвременните военни, политически и икономически кризи са асиметричния характер на въздействията и използването на върховите достижения на информационните и комуникационните технологии. Гарантирането в максимална степен на сигурността и стабилността на общностите, нациите и света изисква разбиране за сигурността като интегрирана система от ценности, способности и готовност. Целта на интегрираната сигурност е да се развива и реализира защитата на жизненоважните социални, политически и финансови мрежи, като същевременно се балансират най-съществените нужди и очаквания за неприкосновеността на личния живот и държавната политика.

Тази мисия взаимодейства с други три стратегически области от национален интерес [1]:

- сигурност на интернет във всичко (Security for the Internet of Everything): свързването на цифровия свят, физическия свят и хората, взаимодействащи с двата свята;
- управление и етика в областта на сигурността (*Governance and Ethics for Security*): въпросите, относно приемането, използването и одита на практиките за сигурност и неприкосновеност на личния живот, които засягат гражданите и правителството, потребителите и бизнеса, както и хората и околната среда.
- анализ на националната сигурност и готовност (*Analytics for National Security and Preparedness*)*:* използване на възможностите на големите данни за подобряване на сигурността, прогнозирането, осведомеността и устойчивостта в отговор на кризи и за националната отбрана.

Сигурността на държавите и регионите се определя в решаваща степен от състоянието на критичната инфраструктура и нейната информационна надстройка. Всяка дейност, операция или транзакция се извършва по електронен път, посредством използването на виртуални услуги в кибер пространството. От сигурността в кибер пространството зависи функционирането на икономиката, военната сфера и цялата обществена система. Поради тези причини кибер сигурността е основен компонент на интегрираната сигурност.

Кибер заплахите имат отличителни характеристики, свързани с цифровата среда. Те са асиметрични, което означава, че злоумишленици с ограничени финансови или технически ресурси могат да компрометират цели с висока стойност. Освен това, атакуващият винаги има предимство във виртуалната сфера. Корпоративната природа на мрежата определя приоритет на откритостта по отношение на сигурността. Тези особености поставят кибер защитата на втори план след офанзивните заплахи, т.е. за да се гарантира сигурността, следва да се предприемат изпреварващи защитни мерки, което не винаги е възможно, поради създаването на нови и нови рискови вектори.

Кибер рисковете определят равнището на сигурност на национално и транснационално ниво. Те се разглеждат в три основни направления:

Кибер престъпления. Това са действията на отделни субекти или организирани групи със злоумишлени намерения за придобиване на ценни данни или парични средства, или за предизвикване на други обществени вреди. Разновидност на кибер престъпленията е *кибер шпионажът* – практиката за използване на информационните канали за придобиване на конфиденциална информация, вкл. патенти, изобретения и ноу хау. Целта в тези случаи е чрез кражба на иновации и интелектуална собственост да се постигне стратегическо предимство.

Кибер война. Това са действията на държава, която извършва саботаж срещу друга държава с цел да предизвика сериозни вреди чрез проникване в компютърните ѝ мрежи, модифициране на данни или разрушаване на комуникациите и/или критичната информационна инфраструктура. Кибер войната се разглежда като петия компонент във военната сфера наред със сухопътния, морския, военно-въздушния и космическия.

Нито една държава не може да се защити напълно успешно от транснационалните информационни заплахи. Кибер атаките могат да станат дори повод за разпалване на конфликти между държави и нарушаване на стабилността. Информационното пространство е трансгранично и не е достатъчно добре защитено посредством международни съглашения и договори. Правят се стъпки в тази насока от страна на международни организации, но процесът е все още в начална фаза. Националното законодателство също няма надеждни лостове за санкциониране на кибер престъпленията. Нещо повече, те са трудно разкриваеми и естеството на технологията дава възможност да бъдат прикрити следите от провеждане на атаката. Високата степен на анонимност на уеб комуникациите прави идентифицирането на нападателя трудоемка, ако не и изключително трудна задача.

Технологията се използва за водене на информационна война, част от която е кибер войната. По този начин в медийното пространство се разпространява дезинформация и се създават определени настроения в обществото, които предизвикват нестабилност.

Информационната война е съществена част от политическото противопоставяне. Тя се провежда преди, по време на и след военната операция. Целта на информационната война е да усили или отслаби резултатите от военната операция или да я неутрализира. Като всяка друга форма на война тя притежава всички характеристики на военните действия: стратегия, тактика, настъпление, отбрана, планиране и щабна работа.

Но за разлика от класическата война, при която отбраната е естествена част от военните действия, при информационната война отбранителните действия може да доведат до поражение. Поради тази особеност, тя следва да бъде винаги активна и настъпателна (*Кедми, 2017*).

Факторът „време“ е от съществено значение. От наличието или отсъствието на информация в реално време зависи успехът на всяка операция. Но освен навременността, от съществено значение е достоверността на информацията. Кибер сигурността означава защита на системите, мрежите и данните във виртуалното пространство.

Заплахите се инициират от хакерски групи, които са обучени да използват уязвимостите в компютърните устройства и софтуера и често действат под покровителството на вътрешни агенти. Този тип атаки могат да нарушат напълно функционирането на мрежата на противника, да преустановят комуникациите или да затруднят дейности, свързани с националната сигурност и отбрана.

В съвременните условия терористичните групировки също максимално се възползват от информационните технологии. *Кибер тероризмът* се свързва с действията на независима организация, която използва глобалната мрежа за своите цели и може да предизвика разрушения в информационната инфраструктура и дестабилизиране на обществения ред и сигурност.

Осъществяването на адекватна защита срещу кибер рисковете във виртуалната среда е сложна и трудна задача. Необходимо е да се създаде ефективна система за защита, която обхваща всички направления за сигурност: персонална, компютърна, комуникационна, физическа и интернет сигурност. Крайната цел е да се съхранят основните характеристики на информацията – тайна, цялостност и наличност.

По отношение на критичната информационна инфраструктура, кибер атаките могат да предизвикат два основни типа поражения [2]:

- каскадни поражения, поради взаимната свързаност на системите за управление на различни сектори;
- ескалиращи поражения, поради зависимостта на системите в рамките на определени процеси.

Поради своята значимост за стабилността на процесите на национално равнище, критичната информационна инфраструктура е цел на злоумишлени атаки от страна на терористични организации или вражески държави. Новите заплахи действат във виртуалното пространство, отвъд географските граници и територии. Компютеризираната инфраструктура може да бъде атакувана чрез уязвимостите в комуникационните мрежи, софтуера или хардуера на системите за управление, с цел блокиране, нарушение или дори физическо унищожаване на критичните компоненти. Идентифицирането на злоумишлениците е трудно и отговорът е насочен не към тях, а към самата организация, мишена на атаката, с цел максимално бързо възстановяване на непрекъснатостта на процесите.

Противодействието на заплахите към критичната информационна инфраструктура включва широк спектър от операции на превенция, възпиране, идентификация и разкриване на атаките, отговор, контролиране на щетите и възстановяване. Тъй като този процес засяга националната сигурност, един от подходите е да се разглеждат основните равнища на управление: стратегическо, оперативно и тактическо. Една гледна точка е представена от *Tabansky*, който дефинира технологично, техническо-тактическо, оперативно и национално-стратегическо равнище.

Тъй като компютърните системи и мрежи са информационна среда, съдържаща технически устройства и технологични софтуерни решения, би следвало да търсим методи и средства за превенция на заплахите от същото естество. Прилагат се технически и технологични мерки за защита в три направления: за превенция (напр. Intrusion Prevention System), за откриване на проникване (Intrusion Detection System) и за възпиране действието на атаките. Съвременните виждания са свързани с резервиране на критични компоненти в компютърните системи, благодарение на което се реализира т. нар. „fault tolerant" принцип. По този начин се постига устойчивост на системите в условията на провеждане на атаки, чрез автоматично заместване на поразените компоненти. Очевидно е, че предлаганият подход води до оскъпяване на технологичните системи, но анализът на съотношението „цена-сигурност" ще даде точна представа за необходимите инвестиции.

Особеностите на системите от критичната информационна инфраструктура също създават предизвикателства пред киберсигурността. В някои от случаите тези сектори (респ. системите) са частна собственост. Освен това трябва да се вземе под внимание фактът, че критичните системи не са от информационно-справочен тип, а са информационни системи за управление на процесите в съответната сфера, т. е. обхватът на системите е широк и включва целия производствен цикъл и услугите, които те предоставят на вътрешните и външните потребители. Системите от критичната информационна инфраструктура имат двойно предназначение – в мирно и във военно време – и поради тази особеност са пряко свързани с националната сигурност и стабилността на обществото. Посочените специфики определят необходимостта да се създаде национална стратегия за киберсигурност, която да съдържа националните приоритети и да регламентира поведението и задачите на всички заинтересовани страни и участници в кибер пространството. В тези условия всяка организация ще определя политиката и инвестициите си за сигурност не само на базата на оценката на риска за своите собствени системи, но и ще се съобразява с регламента, който дефинира стратегическите приоритети в национален мащаб. Като се вземе предвид, че голяма част от организациите са трансгранични, следва да се отчита свързаността и взаимодействието между системите не само на национално равнище, но и отвъд границите, в глобалното виртуално пространство.

Паралелно с дефинираните аспекти на сигурността в кибер пространството, от изключително значение е човешкият фактор. Желаното равнище на сигурност не може да бъде постигнато без участието на субектите, които са съставна част на системите във виртуалната среда. Субектите са пряко свързани както с процеса на защита, така и с процесите на създаване на уязвимости и заплахи.

Заключение

Съвременният свят се характеризира с бързо развитие на информационните технологии, но този процес поражда създаването на нови техники за заплахи, за откриване и използване на уязвимостите на системите в кибер пространството. Проблемите на сигурността надхвърлят рамките на организациите, взаимодействието между тях и потребителите и клиентите. Съществуват юридически предизвикателства в сферата на кибер престъпленията и необходимост от регламенти с цел санкциониране на опитите за измами и злоупотреби в интернет.

Критичната информационна инфраструктура се нуждае от сигурна защита, поради съществеността ѝ значение за националната сигурност и стабилността на обществото. Тази защита се осъществява посредством активни действия на няколко равнища, най-съществените от които са:

- въвеждане на технически и технологични средства за гарантиране на информационната сигурност в системите, принадлежащи на кибер пространството;
- създаване и изпълнение на оперативни процедури за защита на системите и мрежите на физическо, персонално и организационно равнище при експлоатацията им;
- прилагане на националните стратегии за кибер сигурност, с цел отразяване на взаимните връзки и зависимости между обектите на критичната инфраструктура.

Международната общност в съвременния кибер свят разчита в голяма степен на транснационалното взаимодействие между заинтересованите страни за установяване на доверие и споделяне на информация за кибер заплахите в общ интерес. Процесът за сигурност ще бъде подкрепен и чрез създаване на законова рамка и регулатори за ограничаване и санкциониране на нарушенията и престъпленията в кибер пространството.

Библиография

1. Hume center for national security and technology, http://www.hume.vt.edu
2. Cyberspace and national security, Issue of Institute for national security studies, 2013
3. Tabansky L., International cooperation in critical infrastructure protection against cyber threats, Atlantic voices, v. 2, issue 9, 2012
4. Masters J., Confronting the cyber threats, Council on foreign relations, 2011
5. Каракънева Ю., Киберсигурност, изд. Авангард Прима, 2013.

Автор

доц. Юлияна Каракънева – Нов български университет