ПЛАНИРАНЕ НА СПОСОБНОСТИ ЗА КИБЕРСИГУРНОСТ

Венелин Георгиев

CYBERSECURITY CAPABILITY PLANNING

Venelin Georgiev

Abstract: *The report is based on two key assumptions: the growing importance of cybersecurity as one of the essential aspects of the security of its various levels and the need for cyber capabilities building which are adequate to rapidly changing threats and cyber attacks. There are examples of good practices for concepts, processes and strategies for planning capabilities for cybersecurity.*

Keywords: *planning, capabilities, scenario, cyber security, capability gaps, cyber security strategy*

В рамките на последното десетилетие проблемите, свързани с киберсигурността се превърнаха в глобален приоритет за всички, които по един или друг начин имат отношение към проблемите на сигурността като цяло. Без съмнение не могат да съществуват каквито и да било организации, в това число правителствени, неправителствени, частни, образователни, изследователски и т.н., чиято сигурност да не е свързана и да не зависи от сигурността на техните компютърни системи и мрежи, от лоялността на пресонала, който работи с тези системи и мрежи и от свързаните заплахи, рискове и атаки. Използването на съвременните бързоразвиващи се информационни технологии дава предимства на организациите по отношение на тяхната конкурентност, но едновременно с това идват и недостатъците от недоброна- мереното използване на същите тези технологии срещу сигурността на същите тези организации. Практиката показва, че заплахите за киберсигурността под формата на кражба на данни, кибератаки на компютърните системи и мрежи и други непрекъснато нарастват по мащаб и интензивност като едновременно с това се модифицират. По данни от проведено изследване годишните загуби, които киберпрестъпността нанася в глобален мащаб са от порядъка на 114 млрд американски долара.

Според някои автори, все още не е преодоляно времето на съществените трудности както пред справянето с предизвикателствата на

киберзаплахите, така и пред самото дефиниране на киберсигурността. Други автори, занимаващи се с въпросите на киберсигурността, поддържат мнението, че днес въпросът за дефиниране на рамката, в която следва да се търсят и обясняват различните аспекти на киберсигурността и на способностите за нейното осигуряване на практика е решен.

Провежданите изследвания в областта на киберсигурността позволяват определяне на съществуващите способности за киберзащита както и предвиждане на необходимите бъдещи способности предвид на измененията в киберпространството и развитието на организациите и на начините, по които те оперират. На тази база става възможно определяне на липсите на способности (capability gaps) за осигуряване на киберсигурност и създаване на стратегии за тяхното преодоляване. Всичко това става в рамките на процеса за планиране на способности в интерес на поддържане на желаното ниво на киберсигурност.

Намирането на подходящи решения за елиминиране на липсите от способности за киберсигурност е свързано с намирането на отговори на следните въпроси:

Нуждае ли се киберсигурността от процес за планиране на необходимите способности? На този въпрос може да се отговори със следния пример: загубите, нанесени от киберпрестъпността за последната година в парично изражение са нараснали с 56% спрямо предходната като тенденцията е същите тези загуби да нарастват в годините с бързи темпове в случай, че не се разполага със способности преди всичко за превенция, а също така и за възстановяване на последствията от успешните кибератаки. Тези факти са доказателство за необходимостта от изграждане и поддържане на пакети от способности за киберсигурност, което да бъде резултат от прилагането на един рационален и достатъчно ефективен планиращ процес. Нещо повече, бързата промяна и динамичният характер на заплахите за киберсигурността правят изграждането и поддържането на необходимите способности за киберсигурност твърде значимо предизвикателство. Като пример, динамичният характер на киберпространството създава непрекъсната липса на актуални способности за справяне с най-новите киберзаплахи. Рационалният процес за планиране на способности за киберсигурност би допринесъл за възможностите на организацията да „вижда" по-далече в бъдещето и изпреварващо да изгражда онези способности, които ще бъдат адекватни на очакваните бъдещи заплахи за киберсигурността.

Какви са най-добрите практики за планиране на способности за осигуряване на киберсигурност? Независимо от специфичните особености на използвания планиращ процес, същият следва да бъде изчерпателен в своето съдържание, осигуряващ високо качество и итеративност. Технологиите на планиращия процес трябва да позволяват предвиждане

(не прогнозиране) на развитието на организацията, на промените в киберпространството и на заплахите за киберсигурността.

Какви организационни и управленски структури и подходи, а също така и каква информация се използват при планирането на способности за киберсигурност? Бързите промени, настъпващи в киберпространството и в заплахите за киберсигурността на организациите често пъти стават причина за това организациите да не успяват да планират точните способности за гарантиране на своята киберсигурност или да изграждат способности, които вече не отговарят на актуалните заплахи за киберсигурността. Като резултат от това се получава ниско ниво на киберзащита и липса на желаната киберсигурност, от което са застрашени целите на организацията.

Притежава ли киберсигурността уникални характеристики, които да оказват влияние върху същността и съдържанието на процеса за планиране на способности в нейн интерес? Способностите в интерес на киберсигурността следва да бъдат достатъчно гъвкави за да се прилагат срещу променящите се заплахи, но в същото време се налага да притежават достатъчна устойчивост и надеждност, което да гарантира тяхната ефективност в условия на заплахи или атаки срещу киберсигурността. Заплахите за киберсигурността непрекъснато се променят за сметка и в резултат от навлизане на нови технологии и повишаване на способностите на киберпрестъпниците. В тези условия на организациите се налага да „виждат" в бъдещето, да разпознават новите заплахи за киберсигурността и да изграждат необходимите способности за справяне с тях.

Като обобщение може да се каже, че способностите с които организацията разполага следва да позволяват своевременна, точна и достатъчно ефективна реакция срещу кибератаките в различни ситуации и за различни времеви периоди. Изграждането на пакет от способности за киберсигурност, който да отговаря на горните изисквания освен всичко друго се нуждае от прилагане на подходящ процес за тяхното планиране.

При планирането на способности за киберсигурност на организацията могат да бъдат използвани различни подходи. Достатъчно рационалният подход за планиране на способности за киберсигурност следва да предоставя възможности за разкриване и анализ на рисковите области и да позволява на организацията правилно да разпределя ресурсите за посрещане на предизвикателствата от промените в средата и начина й на оперираие. Без съмнение при планиране на способностите за киберсигурност на организациите ще ми бъде нужен подход, който да отчита техните специфични особености и свързаните с тях изисквания към способностите за киберсигурност.

Различните организации прилагат различни подходи при планиране на необходимите им способности за киберсигурност, което не може да се приеме като изненада предвид на това, че не съществува единствен и общоприет подход за тази цел. Като следствие, на всяка организация й се налага да прави избор за подход за планиране на необходимите способности за киберсигурност.

В общия случай добрите практики за подходи за планиране на способности за киберсигурност могат да бъдат структурирани на две нива и включват в своето съдържание компоненти и съответните им елементи, които са представени в схематичен вид на фигура 1.

Компонент			
Елементи	***Процес:*** Изграждане на интегрирани и логични средства за идентифициране на рисковете и потребностите за кибер сигурност	***Стратегия:*** Осигуряване на пряка връзка между дейностите и необходимите способности за киберсигурност	***Инфраструктура:*** Поддържане на изпълнението на достатъчно ефективен и надежден процес за планиране на способности за киберсигурност
	Модел: Дефиниране на единен планиращ процес, която е част от процеса на стратегическо управление ***Данни:*** Определяне на смислени, надеждни количествени и качествени данни за целевите оценявания и решенията на проблемите ***Анализи:*** Базират се на разнообразни техники за моделиране и анализ, визуализиране и оценяване на изискванията, организиране и структуриране на данните за идентифициране на рисковете и информирани решения	***Визия:*** Осигуряване на дългосрочен поглед за стратегическите направления и цели пред организацията ***Управление:*** Осигуряване на прозрачно и отчетно вземане на решения, както и на процеси и структури, които превръщат решенията в действия ***Изпълнение:*** Извършване на непрекъснат мониторинг, оценяване и приоритизиране на дейностите за балансиране с изискванията	***Хора:*** фокусиране върху подходящи знания, умения и практически опит ***Сътрудничество:*** Комбиниране на „top-down" и „bottom-up" подходи за участие, даващи възможности за управление на знанието ***Технологии:*** Изграждане и поддържане на информационни и аналитични системи, поддържащи процеса за планиране на способности за киберсигурност

Фиг. 1. Компоненти и елементи на добрите практики при подходите за планиране на способности за киберсигурност

Оценяването на всеки от компонентите на фиг. 1 включва задълбочен анализ на стъпките на процеса за планиране на способностите за киберсигурност. В общия случай този процес включва следните четири стъпки:

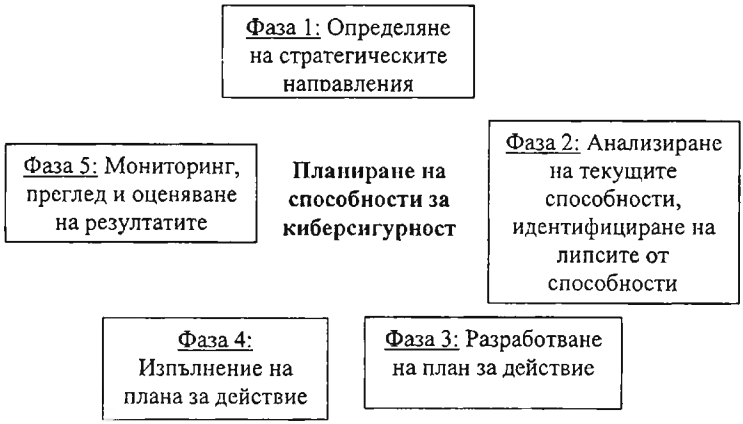
- Процесът за планиране на способности за киберсигурност започва с определяне на текущите способности за киберзащита, описани с помощта на подходящи техни характеристики, които са както общи така и специфични за конкретната организация.

- Като втора стъпка в процеса се извършва анализ на изискванията към бъдещите способности за киберсигурност чрез изследване на организационните цели и стратегическите направления пред организацията и промените в средата, в която тя оперира.

Третата стъпка на процеса включва идентифициране на липсите на способности за киберзащита чрез сравняване на необходимите с текущите способности. Тук се включва и определяне на действията, които следва организацията да предприеме за елиминирането на липсите на способности за киберзащита.

- На следващо четвърто място се изготвя план за съвкупност от дейности с детайлизирани стъпки, изпълнението на които води до изграждане на необходимите способности за киберсигурност и елиминиране на иденитифицираните липси на способности.

Прегледът на различни методики за планиране на способности за киберсигурност дава възможност за представяне на една обобщена схема, включваща фазите от съдържанието на планиращия процес (виж фиг. 2) [2].



Фиг. 2. Фази от методиката за планиране на способности за киберсигурност

Съдържанието на отделните фази на методиката, показано на фиг. 2 може да бъде конкретизирано по следния начин:

- фаза 1: В рамките на тази фаза се извършва оценяване на стратегическия план на организацията и идентифициране на целите, даващи представа за това как ще изглежда организацията и как тя ще оперира в бъдещето. На тази база се определя пакета от способности за киберсигурност, които са необходими на организацията по пътя на нейното развитие.

- фаза 2: Извършва се преглед и анализ на качествените и количествените характеристики на текущите способности за киберзащита на организацията. На тази база се идентифицират липсите на способности за киберсигурност.

- фаза 3: Разработване на план за действие, чието изпълнение позволява приоритетно преодоляване на липсите на способности за киберсигурност и който е ресурсно информиран и ресурсно ограничен. Тук се прави избор и на подходящи измерители за измерване изпълнението на плана и постигане на целите на организацията.

- фаза 4: Изпълнение на плана за действие в рамките на зададените времеви и ресурсни параметри. В рамките на тази фаза, с помощта на избраните измерители се определят и оценяват получаваните резултати.

- фаза 5: Съдържанието на тази фаза включва оценяване на получаваните резултати от изпълнението на плана за действие, както и намиране на отговори на въпросите и предизвикателствата във връзка с измененията на средата за изпълнение на плана.

Както вече беше отбелязано изясняването на процеса за планиране на способности за киберсигурност изисква по-детайлен анализ на компонентите и елементите, показани на фиг. 1. По отношение на елемента „данни" различните организации и в различните методики могат да бъдат открити някои различия по отношение на подхода за събиране и използване. Всяка от изследваните методики обаче предполага събиране на нужните за планиращия процес данни в рамките на отделните фази на неговото съдържание. Разликата идва от това, че в едни от случаите се разчита предимно на емпирични данни, придобити от анализа на мисията, визията и стратегическите цели на организацията, докато в други случаи се залага на използване на готови бази от данни. Обяснение за описаната разлика може да се търси в спецификата на отделните организации и възможностите им за достап до различни информационни източници.

При всяка от изследваните методики се открива аналитична част, включваща анализ на риска за киберсигурността, анализ на липсите от способности за киберзащита (явяващи се разлики между необходимите в бъдещето способности и разполагаемите в настоящето такива), стратегически анализ и т.н. Включването в съдържанието на методиките на

концепцията за управление на риска позволява на организациите да определят значимите (неприемливите) рискове за киберсигурността, да подберат подходящи стратегии за снижаване на тези рискове и да включат подходящи действия за изпълнението на избраните стратегии в разработвания план за действие.

Като обобщение може да се каже, че познаването и разбирането на съдържанието на компонентите модели, данни и анализи са критични по отношение на избора на подходящ процес за планиране на способностите на организацията за киберзащита. Върху качеството на планиращия процес значително влияние оказват оценяването на риска и анализа на липсите на способности за киберсигурност. В условията на непрекъснато модифициране на заплахите за киберсигурността от особена важност е процеса на непрекъснат мониторинг и контрол на процеса за планиране.

Вторият компонент от фигура 1 „стратегия" включва елементите визия, управление и изпълнение. Всяка успешна организация разполага с визия, която спомага за представяне на нейната мисия и споделяните ценности. Във визията на организацията трябва да бъде отразен въпроса за планиране на способности за киберсигурност, което намира израз в управлението и изпълнението на дейности за изграждане на тези способности, отговарящи на дефинираните изисквания. Визията за планиране на способности за киберсигурност освен всичко друго осигурява общ език и таксономия при определяне на необходимите способности. Изграждането и поддържането на необходимите на организацията способности за киберсигурност изисква прилагането на подходящи форми за управление на планиращия процес, който включват политики, процеси и процедури, засягащи начина, по който дейностите в организацията се насочват, администрират и контролират.

Третият компонент от модела на добрите практики за планиране на способностите за киберсигурност е инфраструктурата и той включва елементите хора, сътрудничество и технологии. Доказано от практиката е, че добрият подход за планиране на способностите за киберсигурност зависи от степента на взаимодействие и свързаност между отделните фази на процеса. Хората са онези, които определят както структурата на планиращия процес, така и начините за взаимодействие и сътрудничество вътре в него. Наличието или липсата на подходящи технологии може да спомогне или да попречи за постигане на желаното качество при планиране на способностите за киберсигурност на организацията. При всички случаи обаче фокусирането върху хората и взаимодействието между тях е от критично значение за ефективността на процеса за планиране на способности за киберсигурност. Технологиите също играят важна роля, но само при отчитане на тяхното бързо развитие и

специфичният им принос спрямо особеностите на конкретната организация.

ИЗПОЛЗВАНА ЛИТЕРАТУРА:

1. National Initiative for Cybersecurity Education. Best practices for planning a cybersecurity workforce. White Paper. 2012

2. Георгиев В. Планиране за способности на базата на сценарии. София, Авангард, 2013

Адрес за кореспонденция:
Доц. д-р Венелин Ангелов Георгиев
Нов български университет
Департамент „Национална и международна сигурност"
София, ПК 1618, ул. Монтевидео №21
0888 256 448 vgeorgiev@nbu.bg