Прагматичен подход за оценяване на метрики за киберсигурност

професор д-р Венелин Георгиев

Резюме: За нуждите на измерването на степента на киберсигурност в организацията се използват метрики, разбирани като инструменти за опосредстване вземането на решение и подобряване на производителността и понятността чрез селектиране, анализ и докладване на релевантна информация. Ефективността на метриките за киберсигурност може да бъде определена с помощта на метаметрики, стоящи в основата на т.нар. „прагматичен“ метод, задаващ стандартни критерии за измерване на ефективността от конкретни метрики за киберсигурност. В доклада се представят резултатите от разработването на технология за прилагане в практиката на „прагматичния“ метод за оценяване на метрики за киберсигурност.

Ключови думи: киберсигурност, метрики, метаметрики, „прагматичен“ подход, измерване, ефективност.

Abstract: For the measurement of the cybersecurity capabilities level, the organization uses metrics, understood as tools to mediate decision-making and improve performance and understanding by selecting, analyzing, and reporting relevant information. The effectiveness of the cyber-security metrics can be determined by meta-metrics that are the basis of the so-called “pragmatic” approach and give setting of standard criteria for measuring the effectiveness of the specific cyber-security metrics. The report presents the results of developing technology for the implementation of the “pragmatic” approach for assessing cyber-security metrics.

Key words: cybersecurity, metrics, meta-metrics, “pragmatic” approach, evaluation, effectiveness.

За управлението на процесите, свързани с киберсигурността е вярна класическата триада от мениджмънта, която казва, че за да бъде управляван един процес е необходимо да бъдат измервани получаваните резултати, което от своя страна изисква познаване и описание на управлявания обект. За нуждите на измерване на резултатите от процесите за киберсигурност се избират адекватни метрики като едно от изискванията към тези метрики е оценяване на тяхното качество и ефективност. В практиката е намерило приложение използването на т.нар. метаметрики, с помощта на които се оценява качеството и ефективността на използваните метрики в сферата на киберсигурността. Метаметриките могат да бъдат дефинирани като информация за метрики или по-точно като метрики за самите метрики.

Широко разпространен в практиката е намерил т.нар. „прагматичен“ подход за периодично подобряване на съществуващи метрики за киберсигурност, който с малки промени може да бъде прилаган при измерването и на други аспекти от дейността на организацията. Посредством „прагматичния“ подход могат да се проверяват предварително кои метрики в киберсигурността са осъществими, полезни и ценни. С други думи – прагматичният подход задава стандартни критерии за измерване на качеството и ефективността от метриките за киберсигурност.

Скала за оценяване на ефективността на метриките за киберсигурност с помощта на „прагматичния“ подход

На фигура 1 са представени девет метаметрики от съдържанието на т.нар. „прагматичен“ подход, които се използват като критериите за ефективност при създаването и обновяването на която и да е метрика за киберсигурност.

За нуждите на изследването на възможността за прилагане на „прагматичния“ подход при оценяване на ефективността на метриките за киберсигурност се използва четиристепенна скала. Избраната скала дава възможност за извършване на измервания в проценти като четирите нива отговарят съответно на ефективност, равна на 0%, 33%, 66% и 100%. За всеки от критериите на „прагматичния“ подход и за всяка от степените на скалата е предложено описание на изискванията към съответната метрика, които дават основание тази метрика да получи конкретна оценка по всеки от показателите на „прагматичния“ подход.

Като пример е разгледано описанието на скалата и възможността за оценяване на ефективност-

Фиг. 1. Метаметрики, изпълняващи ролята на критерии за оценяване на ефективността на метриките за киберсигурност

та на която и да е метрика за киберсигурност по критерия „достатъчно предвиждаща ли е оценяваната метрика“:

0% – метриката е историческа и базираща се на резултати от миналото. Резултатите от измерванията с нейна помощ не могат да послужат за формиране на предвиждания относно състоянието на киберсигурността на организацията;

33% – по принцип метриката е историческа, но дава някакви индикации за бъдещето на базата на „слаби“, недостатъчно доказани тенденции;

66% – метриката определено предоставя предвиждащи възможности на базата на „силни“ тенденции, но също така съществуват съмнения и вариативност;

100% – метриката предоставя високи предвиждащи възможности; обективна е и притежава индикативност за бъдещи условия със силна връзка причина-следствие.

По аналогичен начин, с помощта на същата скала и метаметриките от фигура 1, може да бъде оценена изследваната метрика за киберсигурност по отношение на нейната релевантност, действеност, истинност, разбираемост, прецизност, своевременност, независимост и икономичност.

Оценяване на метриките за киберсигурност с помощта на критериите от „прагматичния“ подход

За да бъде демонстрирано как работят т.нар. „прагматичен“ подход и описаната по-горе скала, се използва примерен модел на технология за оценяване на ефективността на метриките за киберсигурност, който включва четири стъпки.

Стъпка 1: Определяне на целите на измерването. На първо място следва да се определи какви са очакванията от използването на избраната метрика. Нека използваме следната ситуация: достатъчно важен, но често пъти неправилно пренебрегван аспект на киберсигурността е свързан със степента, до която мениджърът на отдела по киберсигурност отговаря на очакванията към него и ръководения от него отдел от страна на потребителите. Ако дейността на отдела се приема по-скоро като препятствие пред бизнес процесите на фирмата, което не е рядко срещан случай, то отношението към киберсигурността ще бъде по-скоро негативно. Още по-учудващо е, че при подобни обстоятелства една малка част от мениджърите по киберсигурност се опитват да определят как стратегическият мениджмънт на фирмата, акционерите и потребителите на услугите на отдела оценяват техните усилия и усилията на ръководения от тях екип. Ако се познават очакванията и изискванията на потребителите е възможно да бъдат предприети мерки за тяхното удовлетворяване и точно тук е мястото на метриките за оценяване на отношението на потребителите към усилията на отдела по киберсигурност. Целта в конкретния случай е да бъдат измерени изискванията, очакванията и потребностите на потребителите на продукта киберсигурност. На базата на резултатите от измерванията с помощта на метриката се дава възможност на мениджъра по киберсигурност да бъде проактивен и да прави по-успешен ръководения от него отдел.

Стъпка 2: Конкретизиране на метриката. Конкретизирането на метриката, която да бъде използвана за оценяване на отношението на потребителите към работата на отдела за киберсигурност изисква намирането на отговори на някои въпроси, сред които попадат следните: до каква степен потребителите са удовлетворени от работата на отдела по киберсигурност и в частност от неговия мениджър; нараства или намалява във времето степента на удовлетвореност (неудовлетвореност) на потребителите към работата на отдела по киберсигурност и т.н. Непосредственото конкретизиране на разглежданата за нуждите на примера метрика може да стане на базата на принципа: „измерване на правилните неща, докладване на резултатите на правилните хора, в правилния формат и в правилното време“:

– Кои са правилните неща, които трябва да бъ-

дат измерени: в случая това са отношението и очакванията на потребителите от дейността на отдела за киберсигурност. Релевантни въпроси в случая са: кои точно са потребителите на продуктите на киберсигурността; с какво са свързани техните очаквания и изисквания. Конкретизирането на метриката изисква отговор едновременно и на двата въпроса.

– Кои са правилните хора, на които трябва да бъдат докладвани резултатите от измерванията: в случая това е мениджърът на отдела по киберсигурност. Индиректно тази информация се оказва полезна и за други служители на компанията, като пример на стратегическия мениджмънт.

– Коя е правилната форма за докладване на резултатите от измерванията: тук се има предвид формата за провеждане на анализ на резултатите от измерванията и формата на самия доклад. Възможен вариант е графическото представяне на резултатите, показващи отношението и очакванията на потребителите на продукта киберсигурност, както и изменението на тези резултати във времето. За да се създаде времеви ред е необходимо да бъдат проведени няколко последователни измервания с помощта на метриката, резултатите от които могат да бъдат нанасяни в съответни таблични форми.

– Кое е правилното време за провеждане на измерването и за докладване на резултатите: ако допитването се извършва твърде често това би могло да затрудни и отблъсне участниците в него. За целта може да бъде разработен времеви график за измерванията, който да бъде съобразен с възможностите на участниците в измерването. Поднасянето на данните от измерването също трябва да бъде съобразено с времето и възможностите за тяхното възприемане и осмисляне.

Стъпка 3: Създаване (формулиране) на метриката. При създаване на конкретната метрика се препоръчва прилагане на структуриран подход и създаване на въпросник за оценяване на очакванията и изискванията на потребителите към работата на отдела за киберсигурност. В този въпросник могат да бъдат включени следните въпроси:

– Оценявате ли като компетентни служителите от отдела за киберсигурност на базата на обслужването, получено от тях?

– Бяхте ли обслужени качествено, с необходимото внимание и уважение?

– Достатъчно ефективни ли бяха взаимоотношенията ви със служителите от отдела по киберсигурност?

– Получихте ли достатъчно изчерпателни отговори и инструкции по интересуващите ви въпроси, свързани с киберсигурността?

Стъпка 4: Оценяване на формулираната метрика с помощта на критериите от „прагматичния подход“ и описаната в предходната част скала. Качеството и ефективността на създадената метрика се оценява последователно по всеки от критериите на „прагматичния“ подход:

– Предвиждаща ли е метриката: избраната метрика помага да се определи/предвиди какво трябва да се промени в отдела по киберсигурност за да се подобрят отношенията с потребителите в бъдеще. Връзката между причините и следствията не е перфектна, като дори при възможно най-висока оценка от страна на потребителя не може да се изключи възможността от възникване на инцидент с киберсигурността, т.е. мнението на потребителите не е силен индикатор за цялостното състояние на киберсигурността във фирмата. Това дава основание по този критерий метриката да получи оценка 66%.

– Релевантна ли е метриката към целите на измерването: създадената метрика осигурява релевантна информация за мениджъра на отдела по киберсигурност, но в същото време не изчерпва тази информация. По този критерий оценката за метриката отново е в средата на скалата – 66%.

– Води ли до конкретни действия (действена ли е) избраната метрика: ако резултатната стойност от оценяваната метрика е ниска, то очевидно следва нещо да се направи, но какво точно трябва да се направи не може точно да се определи на базата на резултатите от самата метрика. При това положение оценката на метриката по този показател е ниска, т.е. под 33%.

– Истинска ли е метриката: информацията, получена с помощта на метриката след анкетиране на потребителите е индикативна и зависи от множество фактори, сред които начин за съставяне и провеждане на анкетата, характерни особености на анкетираните и т.н. И по този показател оценката на метриката е ниска, под 33%.

– Достатъчно разбираема ли е метриката: избраната метрика е разбираема за мениджъра на отдела по киберсигурност, който за да бъде успешен трябва да отговаря на очакванията на потребителите, което на практика означава, че трябва да познава тяхното отношение и очаквания. По този показател оценката на метриката е висока, над 66%.

– Достатъчно прецизна ли е метриката: използваната в интерес на метриката скала с ограничен брой степени донякъде лишава измерванията от статистическа прецизност, но от друга страна конкретното измерване не се нуждае от по-висока прецизност. По-важно в случая е, че метриката дава възможност за извършване на оценяване, както и възможност за проследяване на изменението на оценките във времето. Избраната скала дава възможност за извършване на повторяеми измервания. Оценката по този показател е между 33% и 66%.

– Навременна (своевременна) ли е метриката: по време на използването на резултатите от измерването с помощта на метриката за нуждите на изготвянето на доклада, взаимоотношенията между мениджъра по киберсигурност и потребителите ще продължат да се развиват. Това прави невъзможно повлияване върху текущите взаимоотношения, но възможно коригиране на взаимоотношенията в бъдеще. По този показател оценката е над 66%.

– Независима ли е метриката: възможно е в хода на анкетата по прилагане на метриката да се въздейства върху мнението на анкетираните в посока към постигане на по-добри резултати. Това не рядко се случва в практиката и като следствие прави метриката не много независима. Оценката в случая е под 33%.

– Евтина ли е метриката: разходите за анали-

зиране на данните от измерванията под формата на времеви ред не са особено високи – от 1 до 2 часа на месец за събиране, нанасяне и обработване на данните. Оценката по този показател е над 66%.

На базата на оценките на метриката по отделните показатели се определя окончателната оценка, например като средна стойност от частните оценки. Можем да приемем, че крайната оценка на метриката от примера е между 50% и 60%. В случай, че тази стойност на оценката удовлетворява измерващия, то той може да включи метриката в прилаганата система от метрики за измерване на киберсигурността.

Друг начин за използване на „прагматичния" подход и показателите за оценяване е при сравняване на две или повече метрики, които да бъдат прилагани в дадена област на киберсигурността. След преминаване на оценяващия процес, всяка от метриките получава средна оценка и потребителят на системата от метрики може да избере онази, чиято оценка е с най-висока стойност.

Жизнен цикъл на система от метрики за измерване на киберсигурността

Един по-кохерентен подход за използване на метриките в контекста на управление на бизнеса и на свързаната с него киберсигурност включва проектиране, внедряване, използване и развитие на адекватна система от достатъчно ефективни метрики за киберсигурност. От подобна система се очаква да отчита всички релевантни аспекти на киберсигурността, без да се допускат съществени пропуски в обхвата или да се правят значими ограничения относно нейната приложимост. Създаването на такъв тип система представлява процес, който преминава през определени етапи, наричан още жизнен цикъл на система от метрики за управление на киберсигурността. По своето съдържание този жизнен цикъл може да варира от гледна точка на неговата детайлност, при опита да бъдат обобщени различните варианти се достига до модел, показан по-долу:

- фаза 1: определяне и конкретизиране на изискванията към процеса за измерване;
- фаза 2: разработване на бизнес казус или бизнес решение;
- фаза 3: проектиране на системата за измерване;
- фаза 4: разработване на конкретни метрики;
- фаза 5: тестване на създадената система от метрики;
- фаза 6: внедряване на системата от метрики за измерване на киберсигурността;
- фаза 7: използване и поддържане на системата от метрики;
- фаза 8: развитие на системата от метрики за измерване на киберсигурността.

В рамките на фаза 1 се определят и конкретизират изискванията към процеса за измерване като това се прави на базата на изучаване на потребностите на фирмата, изискванията към системата за измерване и включените в нея метрики; стратегическите, тактическите и оперативните цели на фирмата по отношение на киберсигурността, управлението на риска, общото ръководство и т.н. Като правило, киберсигурността представлява област, която трудно се поддава на измерване и като следствие от това - на управление. Двата съществени момента включват как да се измери риска за киберсигурността и как да се измери снижаването на този риск в следствие на приложените стратегии за противодействие, като пример чрез намаляване на броя и интензивността на инцидентите с киберсигурността. Измерването и проследяването на измененията в броя на инцидентите с киберсигурността може да послужи при доказване на ефективността на направените инвестиции в тази посока. Намаляването на броя на инцидентите с киберсигурността може да означава също така и че атакуващите за момент са съсредоточили своето внимание към други жертви. Обратното също е вярно. Ако броят на инцидентите с киберсигурността нараства, това не означава непременно, че стратегиите за сигурност са се провалили. Нарастването може да се дължи на нарастване на заплахите, използване на по-голям брой съществуващи уязвимости и т.н.

Фаза 2 от жизнения цикъл се свързва с разработване на бизнес казус или бизнес решение. Сърцевината на тази фаза се състои в определяне, аргументиране и осигуряване на необходимите инвестиции за създаване, внедряване и използване на система от метрики за измерване на киберсигурността във фирмата на базата на очакваните ползи/ефекти и разходи.

Във фаза 3 се проектира система за измерване на киберсигурността. С помощта на традиционен архитектурен подход и на базата на оценки с помощта на метаметриките от прагматичния подход, се подбира съвкупност от метрики, всяка от които допринася за ефекта на процеса за измерване. При проектирането на системата за измерване на киберсигурността следва да се отчита начинът, по който метриките ще си взаимодействат в рамките на и извън системата, как ще се допълват взаимно, както и с метрики, измерващи други бизнес процеси.

В рамките на фаза 4 се разработва системата от метрики за измерване на киберсигурността. Тук на практика започва оформянето на системата от гледна точка на описание на процеса за измерване, събиране и анализиране на данните, определяне на начините за визуализиране и представяне на резултатите. За всяка метрика трябва да бъдат определени източниците на данни. Ако за една метрика са необходими голямо количество данни добре е процесът за тяхното осигуряване да бъде автоматизиран. На този етап се обмислят също така начините за обобщаване на информацията и представянето ѝ във вид улесняващ управлението. За метриките, не изискващи голям обем данни (тези, които са опростени и се използват често) може да се приеме ръчно събиране на необходимите данни при положение, че се запази баланса между ползи и разходи.

Фаза 5 е предназначена за тестване на системата от метрики за измерване на киберсигурността. Всяка сложна система изисква да бъде проверена и

нейната работоспособност да бъде доказана, което е вярно и за системата за измерване на киберсигурността. В тази фаза се включва създаването на прототип на системата, провеждане на пилотни изследвания и измервания, проверка на адекватността на метриките, прецизиране на компонентите за анализ и визуализиране. Проверката на системата и нейните процеси в лабораторни условия позволява да се получи нужната увереност за тяхната работоспособност и в реална среда. В хода на тази проверка може да се потърси обратна връзка от потребителите доколко функционалностите на системата отговарят на техните очаквания и нужди. Тази, както и предходните фази от жизнения цикъл на системата за измерване на киберсигурността са до някаква степен итеративни.

При фаза 6 разработената система от метрики за измерване на киберсигурността се внедрява в практиката, което по своето съдържание може да се разглежда като дейност от областта на управление на промяната. Тази фаза включва следене за недопускане на конфликтни промени в други бизнес процеси и функции; подготовка на потребителите на системата от метрики; постигане на увереност, че системата работи нормално, т.е. метриките и измерванията отговарят на потребностите; разработване на план в случай, че системата създава проблеми, който може да включва промяна на метриките или на процесите за измерване.

Фаза 7 включва използване, управление и поддържане на системата от метрики за измерване на киберсигурността. Типични за тази фаза са дейности като следене на работата на системата и при нужда въвеждане на минимални корекции; оценяване на получаваните резултати от гледна точка на целите на измерванията; управление на промените в системата или в бизнес процесите, които са източник на данни, както и на аналитичните модули, на модулите за визуализиране и докладване; потвърждаване на ползите от използване на системата за измерване на киберсигурността.

Предназначението и съдържанието на фаза 8 е свързано с развитие на системата от метрики за измерване на киберсигурността. Изградената и внедрена система има нужда да бъде развивана и усъвършенствана на базата на натрупания опит и настъпилите промени в потребностите на потребителите. Решение за развитие на системата се взимат след проверка на нейното състояние, което като периодичност се препоръчва да се прави всяка година. Тези проверки могат да включват проверка на ефективността и адекватността на използваните метрики с идея някои да отпаднат, а други (нови) да бъдат включвани в системата; автоматизиране на повече процеси за измерване и дори свързване на системата за измерване на киберсигурността с други измерващи системи на фирмата; актуализиране на съдържанието на системата в отговор на настъпили промени във фирмата; преглед и обновяване на изискванията към системата; търсене на независими оценки за работата на системата и на съществуващи добри практики.

Като правило, при системите за измерване се наблюдава тенденция към постепенно разширяване на обхвата чрез включване на нови и нови метрики, които добавят все по-малка стойност. В практиката е доказано, че по-лесно е да бъде добавена нова метрика към системата, отколкото да бъде извадена метрика, която не носи полза за системата и за фирмата. Полезен подход в подобни случаи е този, наречен „плюс една, минус една“, т.е. въвеждането на нова метрика в системата става само след отстраняване на една от използваните до този момент метрики. Възможен е и друг подход – взимане на решение и изваждане на дадена метрика от системата, при което се следи дали някой ще реагира на направената промяна, кой точно ще реагира и колко настойчива ще бъде реакцията. На тази база се решава дали да бъде върната метриката в системата или същата да отпадне.

Създаването и използването на система от метрики за измерване на киберсигурността на организацията е свързано с възможността за оценяване на ефективността и качеството на включените в системата метрики. Описаният в доклада „прагматичен“ подход и съвкупността от метаметрики правят възможно изпълнението на горното изискване.

Georgiev V., V. Monev. Metriki za kibersigurnost. Sofia: Avangard Print, 2016.
Hayden, L. IT security metrics. The McGraw-Hill Companies, 2010.
Brotby, W., Hinson, G. Pragmatic Security Metrics. Taylor & Francis Group, 2013.
Jaquith, A. Security Metrics. Pearson Education Inc., 2007.