IT4Sec Reports 111
http://dx.doi.org/10.11610/it4sec.0111

Метрики за информационна сигурност в предприятията: Класификация, примери и особености

Веселин Монев

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, март 2014 г.

Веселин Монев, Метрики за информационна сигурност в предприятията: Класификация, примери и особености**,** *IT4Sec Reports* 111 (София, Институт по информационни и комуникационни технологии, март 2014 г.), http://dx.doi.org/10.11610/it4sec.0111.

IT4SecReports 111 „Метрики за информационна сигурност в предприятията: Класификация, примери и особености“ Докладът представя анализ на основни проблеми, свързани с измерването на информационната сигурност в една фирма. Разглеждат се няколко класификации на метрики като се акцентира върху функциите на различните нива от управлението на сигурността. В по-голямата си част работата разглежда положителните и отрицателните страни на по-разпространените метрики за измерване на ИТ сигурността и дава насоките за изработване на собствени. Именно собствените, пригодените към фирмената среда метрики, са тези, които мениджърът по сигурността трябва да създаде и използва за целите на ефективното управление.

Ключови думи: Метрика, информационна сигурност, класификация, риск, матрица, очаквана годишна загуба, фирма, инцидент, измерване, мениджмънт, уязвимост.

IT4Sec Reports 111 “Enterprise IT security metrics: Classification, examples and characteristics“ The report addresses the key issues associated with measuring IT security for private companies. Several classifications of metrics are discussed focusing on the functions of different levels of security management. For the most part, this work examines the pros and cons of common metrics for measuring IT security and provides guidelines for creating own metrics. ‘Own metrics,’ adapted to the corporate environment, are those which security managers have to create and use for the purpose of effective management.

Keywords: Metric, metrics, IT security, classification, characteristics, risk, matrix, expected annual lose, company, incident, measure, management, vulnerabilities

Веселин Монев е студент в магистърска програма „Киберсигурност“ на Нов български университет, София. Работи като „ИТ Инженер“ за Хюлет Пакард в областта на корпоративните сторидж продукти.

ISSN 1314-5614

СЪДЪРЖАНИЕ

I. ВЪВЕДЕНИЕ

Един от най-важните въпроси, на който всеки информационен специалист трябва да отговори, е как ще оценява обекта на своя анализ. Този въпрос съдържа много елементи, чието обяснение, анализиране и оползотворяване се осъществява чрез метриките за информационна сигурност.

Използването на метрики за обясняване и определяне на сигурността в една организация е неизбежно за целите на ефективното управление на информационната сигурност. Въпреки това, както ще стане дума в настоящата работа, не съществува единна схема за създаване на метрики, нито универсални методи за анализ на сигурността.

Статията обхваща една малка част от проблема наречен „метрики за информационна сигурност“ и по-специално неговата класификация и анализ на някои често използвани метрики – техните силни и слаби страни. Както ще се посочи по-нататък, различните организации изискват създаването на пригодени за тяхната структура метрики, поради което по-детайлно ще стане дума за особеностите на т.нар. собствени метрики за сигурност.

Разглеждането на метриките ще акцентира върху гледната точка на главния информационен специалист – този който направлява и осъзнава цялостния процес на защита на информационното пространство в организацията. Тази организация може да е всеки вид частна фирма, но не държавата – особеностите на държавната информационна сигурност са достатъчни като обем и затова заслужават да бъдат разгледани отделно.

Поради обема си отделно могат да бъдат разгледани също процесът на имплементация на метриките за информационна сигурност, темата за изработване и изпълняване на проект за измерване на сигурността, както и да се опишат други техники и методи за анализ, включително да се разгледат различни национални и международни стандарти.

След дефиниране на понятието „метрики за информационна сигурност“ и разглеждане на някои класификации, по-голямата част от настоящия текст ще опише конкретни метрики и детайлизира процеса на създаване на собствени.

II. ДЕФИНИЦИЯ НА „МЕТРИКИ ЗА ИНФОРМАЦИОННА СИГУРНОСТ“ И ОБЩИ ПОЛОЖЕНИЯ

Според *Oxford's American Dictionary*[1] метриката е „Техническа система или стандарт за измерване“. Думата произхожда от средата на XIX век, от френското прилагателно *métrique*, свързвано с понятието „дължина“.

Метриките са инструменти за улесняване на процеса на вземане на решение и за подобряване производителността и яснотата чрез събиране, анализиране и докладване на релевантна информация.

[1] *Oxford American Dictionary*, Oxford University Press, 2013, http://www.oxforddictionaries.com/definition/english/metric?q=metric

Метриките за информационна сигурност могат да бъдат получени на различни нива в една организация и за всеки аспект от нейната сигурност. Детайлни метрики могат да бъдат събирани на различно управленско ниво, в зависимост от размера и сложността на организацията.

Ефективните метрики са специфични, измерими, достъпни, използваеми отново и могат да се извършат за отредено време. За да бъдат употребими метриките трябва да показват степента, в която целите са постигнати и да подпомагат вземането на решение за подобряване на сигурността в организацията.

Има три важни особености, които трябва да бъдат взети в предвид:

1. Степента на трудност за събиране на точни данни.
2. Възможността метриката да бъде изтълкувана погрешно.
3. Нуждата от периодичен преглед на метриките, които се използват.

Посочените особености са общи и не са изчерпателни. Отделни определящи елементи ще бъдат разгледани по-нататък.

III. КЛАСИФИКАЦИЯ НА МЕТРИКИТЕ ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Едни автори разграничават два типа метрики: метрики, служещи за оценка на ползите (вършене на правилните неща) и метрики за измерване на производителността (продължаване на вършенето на правилните неща).

Според друга класификация един модел на метрики за анализ на сигурността се състои от три компонента:

- Измерван обект;
- Целите на измерването;
- Методът за осъществяване на измерването.

Според тази класификация метриките се разделят на:

- Изисквания по сигурността, сред които спецификации, стандарти, контролни цели и профили за защита „Common Criteria[2]“;
- Добри практики;
- Изначална сигурност;
- Метрики, основани на старанието, т.е. на опита;
- Цялостни модели като например NFOSEC Assessment Capability Maturity Model, 2003

Методите за измерване включват:

- Директно тестване (например функционално или тест на проникването);
- Измерване;

[2] Common Criteria, http://www.commoncriteriaportal.org/

- Оценка (например на риска или уязвимостта);
- Упълномощаване;
- Обучения;
- Наблюдение на производителността на системата, като например засичане на нарушители.

Следваща класификация разглежда метриките като абстракция в следните категории: технически, организаторни, операционни и „мозъчна атака“, като последната дава синтез.

Четвърта класификация разделя метриките за сигурност според тяхната функционалност на три категории:

- Метрики за измерване на въвеждането на политики за сигурност;
- Метрики за измерване на резултатите от извършеното (ефективност и ефикасност);
- Метрики за измерване на влиянието на събитията в сигурността върху бизнеса или поставената организационна цел.

Тук ще предпочетем да детайлизираме класификацията на метриките според тяхната функция през призмата на бизнеса.[3] За всяка функция съответства определен набор от метрики, чрез които мениджърът по сигурността търси отговор на поставените цели. По-долу са представени функциите от мениджърска гледна точка и резултатите, които метриките трябва да определят.

Мениджмънт на инцидентите: Колко добре става засичането, идентифицирането, справянето и възстановяването от инциденти в сигурността?

Тук могат да се използват различни метрики, разглеждащи: стойността на инцидентите; средната стойност на инцидентите; средната цена за възстановяване от инцидентите; средното време за разкриване на инцидентите; брой инциденти; средно разстояние за случване на инциденти; средно време за възстановяване от инциденти.

Мениджмънт на уязвимостите: Колко добре се управлява излагането на организацията на уязвимости при идентифицирането и смекчаването им?

Метриките, които могат да се използват, разглеждат: покритие на сканирането за уязвимости; процент на системите с неизвестни съществени уязвимости; средно време за смекчаване на уязвимостите; брой на известните компютри, които имат уязвимости; среден размер на разходите за смекчаване на уязвимостите.

Мениджмънт на пачването: Колко добре се справяме с поддръжката на пачването на системите?

За отговор на този въпрос се използват метрики, които способстват събирането на следната информация: спазване на политиката за пачване; степен на обхващане на пачването от мениджмънта; средно време за пачване; средни разходи за пачване.

---

[3] *The CIS Security Metrics v1.1.0*, Center for Internet Security, November 2010, https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf

Мениджмънт на конфигурирането: Какво е състоянието на системите по отношение на конфигурирането им?

Тук метриките търсят да отговорят на следните въпроси: процент на конфигурираните устройства; степен на покритие на конфигурирането от мениджмънта; текуща политика срещу зловреден софтуер.

Мениджмънт на промените: Как промените в системата се отразяват на сигурността в организацията?

Въпросът може да се измери с метрики, даващи следната информация: средно време за извършване на промените; процент на промените, чиято сигурност е тествана и на промените, които са изключение от тестването.

Сигурност на програмния софтуер: Може ли да се разчита, че бизнес програмите ще работят така, както очакваме?

В случая метриките търсят информация за: броя на програмите; броя на критичните програми; обхват на оценката за риска; обхват на тестването на сигурността.

Финансови метрики: колко средства се отделят за сигурност на информационните системи и за каква цел конкретно?

Метриките търсят стойности за: Какъв е бюджетът за сигурността на информационната сигурност като процент от общия бюджет за информационна сигурност?; Какво е преразпределението на бюджета за информационна сигурност?

Бъдещи функции: Препоръки за допълнителни бизнес функции.

Примерни области за изготвяне на метрики са: данни/информация; цикъл за развитие на софтуер; мениджмънт на конфигурирането; мениджмънт на риска от трета страна; допълнителни метрики за финансите; автентификация и оторизация; сигурност на данните и мрежите; контрол на зловредния софтуер.

Същият документ предлага три категории метрики, в зависимост от тяхното предназначение и аудитория. Метриките за управление са по правило най-важните за организацията, но може да изисква прилагането на базисни технически метрики. Трите категории са представени така:

Мениджърски метрики: дават информация за производителността на бизнес функциите и влиянието им върху организацията. Аудиторията е бизнес мениджмънтът. Метриките търсят стойност на въпроси като: цена на инцидентите; спазване на процедурите за пачване и др.

Операционни метрики: използват се за да се разберат и оптимизират дейностите на бизнес функциите. Аудиторията е мениджмънтът по сигурността. Тук се търси информация за средната стойност за възстановяване от инцидентите; средната стойност за пачване; средното време за пачване; средното време за намаляване на уязвимостите; преразпределение на бюджета за информационна сигурност и др.

Технически метрики: дават технически детайли, както и база за направата на нови метрики. Аудиторията са специалистите по сигурност на операциите. Метриките се отнасят за въпроси като брой на инцидентите, обхват на управлението за пачване, сканиране на

уязвимостите, спазване на процедурите за справяне със зловреден софтуер, брой на програмите, обхват на тестването за сигурността и др.

Настоящата работа счита, че всяка от тези класификации има своите предимства и недостатъци в конкретна среда и при поставени конкретни цели.

IV. НЯКОИ МЕТРИКИ ЗА ИНФОРМАЦИОННА СИГУРНОСТ. ПРЕДИМСТВА И НЕДОСТАТЪЦИ.

За да се разберат метриките за сигурност е необходимо първо да се разбере ролята им в съвременния свят.

Много специалисти по сигурността използват метрики като „Очаквани годишни загуби“ и „Общи фирмени загуби“. Нараства обаче убеждението, че традиционните метрики са недостатъчни, тъй като не дават информацията, от която се нуждаем, за да вземем обмислени решения и да изчислим стойността на мерките за сигурност. Все повече специалисти застъпват мнението, че трябва да вземем в предвид иновативни методи за анализ на метриките.

Информационната сигурност заема важна роля в една фирма и поради това е нужно главният информационен специалист да има глобален поглед не само над процесите и механизмите, които управлява, но и върху зависимостите на фирмата отвън. От тук склонността на много хора да измерват само нещата, с които си имат работа, често се оказва недостатъчно пълен подход.

Метриките са данни сами по себе си и могат да бъдат превърнати в информация, от която да се извлекат знания. Те помагат да се разбере сигурността само ако са сложени в контекст, т.е. знаем какво искаме да направим, след като ги притежаваме. В този смисъл събирането на данни е важно, но не е крайна цел, а средство за анализ.

Измерването на рисковете, което постигаме посредством метриките, трябва да се използва по подходящ начин, защото иначе вложените усилия биха били напразни и дори биха създали у нас чувство на несигурност. Метриките за сигурност трябва да са част от бизнес процеса, който постоянно подобрява защитата на фирмената информация.

Когато се провежда програма за събиране на метрики по сигурността участниците трябва да си дават сметка за ползите и целта, на която те ще послужат. Освен това трябва да се отчетат разходите и ползите от събирането на данни. В крайна сметка този процес трябва да води до създаване на ново знание.

В настоящата работа се приема, че добра метрика е тази, която намалява несигурността в организацията. Тук няма значение дали метриката е количествена или качествена.

Всяко измерване е проблемно, когато не е извършено пълно. То може да съдържа нередности в качеството на данните, емпирични грешки или да се използва по подвеждащ начин.

Долните метрики не са изчерпателни и съдържат един или повече от тези проблеми.

1. МАТРИЦА НА РИСКОВЕТЕ

Рискът е фундаментална концепция в ИТ сигурността и често е недоразбрана, тъй като се използва за описване на много различни феномени. Един често срещан метод е чрез матрицата по-долу:

		Вероятност от събитие		
		Силна	Средна	Слаба
Размер на влиянието	Силно	_____ _____	_____ _____	_____ _____
	Средно	_____ _____	_____ _____	_____ _____
	Слабо	_____ _____	_____ _____	_____ _____

Фиг.1

Тази матрица може да има вариации, стойности или други цветове. Общото между тях е, че изчисляват вероятността за случване на определено рисково събитие и колко лошо ще е влиянието на съответния риск. Таблицата се попълва с рискове с цел приотизацията им.

Това е прост метод за анализ и поради тази причина продължава да се прилага толкова дълго време. Въпреки това таблицата е твърде ограничена, за да поеме голямото количество данни, на базата на които да вземем важни решения по сигурността.

Матрицата не е добра за измерване на текущия риск, но може да послужи ефективно за изграждане на целева база от мнения. Чрез нея експертите по сигурността биха могли бързо да направят прототип на предполагаемо най-големите проблеми в сигурността. Разбира се, мненията тук са различни и може да си противоречат. Тя може да е полезна, но си остава сбор от мнения на експерти. Надеждата тук е, че рисковете в сигурността до определена степен ще съвпадат с посочените рискове на експертите по сигурността. Необходимо е да се прецизират рисковете, за да се ограничи степента на несигурност при избора им. Тук експертът трябва да избягва да попадне в заблуда, игнорирайки умишлено или не идентифицираните факти. В противен случай матрицата може да се бъде заблуждаваща.

Важно е да се уточни, че личната оценка на риска в сигурността не измерва риска. Това е така, защото личности дават своята лична оценка за сигурността, на база на своите субективни наблюдения. Тези наблюдения не винаги съвпадат с това, което е наблюдавано. Подходящо е данните да се използват за фокусиране върху определен диапазон от разпознати рискове, но без да се превръщат в точни цифри.

За улесняване на възприемчивостта на данните е възможно нивата за оценка да бъдат заменени с числови стойности. Тези нови нива образуват *номинална скала*. Така например от представената по-горе матрица можем да заместим нивата на *Размер на*

влиянието – Силно, средно и слабо с – 3, 2 и 1. Това дава и втори положителен ефект - възможността да се направи сборна оценка, като например 2,5.

Въпреки, че една матрица, чиито данни се базират на мнения, може да изглежда, че представя количествени данни, те не измерват фактическия риск. Затова най-доброто приложение на тези таблици би било за обобщаване на мненията на различните експерти в организацията или за измерване на различните мнения.

2. УЯЗВИМОСТИ В СИГУРНОСТТА И СТАТИСТИКА НА ИНЦИДЕНТИТЕ

Анализирането на уязвимостите е важно, но съсредоточаването твърде много върху тях може да създаде страхове и несигурност. В съвремието уязвимостите на една фирма не се показват пред обществото. Нито една фирма, занимаваща се с професионални анализи не може да си позволи да публикува подобна информация, тъй като тя е интелектуална собственост. Поради тази причина изследователите се затрудняват да получат достъп до нея. Това води до невъзможността на една организация да сравнява своите данни с данните на друга.

3. ОЧАКВАНА ГОДИШНА ЗАГУБА

Тази метрика е сред най-използваните. Тя определя колко са предполагаемите загуби в следствие на инциденти в сигурността. Докато оценката на риска, представена преди това ни дава възможност да приоритизираме рисковете качествено, то очакваната годишна загуба ни дава изцяло количествени данни, образувани чрез формули и статистически методи.

Формулата се изразява по следния начин:

ОГЗ = ГСП x ОЕЗ

Очакваната година загуба = Годишната степен на проява ***x*** *Очакваната единична загуба*

Тази формула, подобно на матрицата с рисковете, отново не оценява рисковете, а взема в предвид мненията за стойността на вредите, нанесени при реализация на рисковете. Тук съществува опасността да възприемем формулата като представяща нещата по начин, какъвто ще се случи.

Формулата за очаквана годишна загуба не представя категорична вероятност, тъй като не разполага с всички необходими данни за изваждане на такова стойност. Една от причините за недостига на такива данни е, че организациите нямат процеси и технологии за засичане на уязвимостите и инцидентите в реално време и използването на информацията за тях на по-късен етап.

Друг важен проблем на формулата е, че тя не обхваща загубите, свързани с имиджа на марката или репутацията на фирмата. Освен това паричното измерване на загубите във времето е неточно. Това, което трябва да се разбере е не колко са преките загуби от например неработещия хардуер, а какви са косвените загуби, включително ефективност, продуктивност, конкурентоспособност.

4. ВЪЗВРЪЩАЕМОСТ НА ИНВЕСТИЦИИТЕ

Тази метрика е взета от света на бизнеса и идеята е да се отговори каква е печалбата от вложените усилия.

От гледна точка на сигурността *възвръщаемостта на инвестициите* се споменава в няколко отношения.

Първо, тя се споменава в във връзка с *очакваната годишна загуба*, когато се предприемат мерки срещу очакваната загуба. Например, ако очакваната загуба е на стойност 10,000 лв. и ние инвестираме 2,000 в превенция, то възвръщаемостта би била 8,000 лв. Ако обаче отделим 12,000 лв. в превенция, то възвръщаемостта би била отрицателна: -2,000 лв.

Вторият контекст на приложение на *възвръщаемостта на инвестициите* е при рекламирането на продукти. Например ако даден производител представи как неговият продукт ще намали загубите на дадена фирма чрез увеличаване на ефективността и продуктивността. Този доставчик може да използва тази метрика, за да покаже ползите от продукта си във връзка с цената му.

Метриката *Възвръщаемост на инвестициите* може да бъде използвана и за заблуда, тъй като тя не може да се приложи по идентичен начин в отношението „вложени ресурси – печалба“. Сигурността не може да се разглежда по този начин, тъй като дейностите по сигурността не се разглеждат като център за трупане на печалба (освен ако не са предоставени на някого с бизнес цели). ИТ сигурността говори за превенция на загубите, не за печалба.

Причината ИТ сигурността да бъде представяна като инвестиция е склонността на хората да дават пари на някого, който ще ги увеличи.

Тук проблемът на метриката е като предишните – данните в уравненията са ненадеждни и нещо повече - използват се от маркетолозите в тяхна собствена полза с цел подвеждане на клиента.

5. ОБЩИ ФИРМЕНИ РАЗХОДИ

Докато метриката за *очакваните годишни загуби* се опитват да измери загубите в ИТ системите, а *Възвръщаемостта на инвестициите* – „печалбата“ от тях, то *Общите фирмени разходи* търсят отговор на въпроса колко разходи са необходими през целия жизнен цикъл на продукта или услугата – от покупката до прекратяването на използването. Тази метрика се опитва да отчете следните фактори:

- Главните системни компоненти: хардуер и софтуер;
- Такси за лиценз и поддръжка;
- Необходима инфраструктура (пространство, енергия, контрол над средата);
- Инсталация и поддръжка;
- Обучение и експертиза;
- Сигурност и одит;
- Скрити разходи.

Тази метрика действително дава знания за това колко ще струва покупката на определен продукт за сигурността, но не дава отговор на въпроса дали съответната фирма има нужда от него. Метриката помага да се направят по-информирани избори, но се използва и от производителите да манипулират избора на главния специалист по сигурността на ИТ инфраструктурата на една фирма.

6. СОБСТВЕНИ МЕТРИКИ

6.1. Общи особености

Описаните метрики, както беше споменато, са несъвършени и недостатъчни за разбиране на инцидентите в сигурността. Поради това е необходимо да се изработят собствени метрики. Добрите метрики са не само правилно избраните, но и ефективно пригодените към конкретната среда.

Съществува мнението, че метриките трябва задължително да бъдат количествено представени. В тази работа приемаме, че както количествените, така и качествените метрики имат своето място по въпросите за сигурността.

Метриките са стандарт за измерване. Самите метрики са резултат, а измерването – процес. Чрез измерване могат да се постигнат следните положителни ефекти:

- Предсказване на неща;
- Даване на обща рамка като противоположност на единичния опит;
- Решаване на несъгласия чрез стандартизиране на критериите и ценностите;
- Популяризация на справедливостта чрез изискването всеки да се придържа към еднакви стандарти;
- Прецизиране на описанията и разграничаванията.

В процеса на изработване на собствени метрики е важно да се отговори на няколко въпроса.

Въпрос 1: Разбирате ли метриката?

На този въпрос се търси отговор чрез няколко подвъпроса:

- Причината за измерването. Тя е различна от задачата да се създадат метрики във фирмата въобще.
- Каква е аудиторията, на която ще бъдат представени метриките? Какво трябва да се направи, за да се представят те разбираемо?
- Качествата и характеристиките на програмата за сигурност, която е оценявана.
- Какви наблюдения са направени за целите на метриката и как са направени те? Кой прави наблюденията и как тези наблюдения ще повлияят на метриките?

Въпрос 2: Използвате ли метриката?

За целите на определена метрика се изразходват определени ресурси. Поради тази причина специалистът трябва да си зададе въпроса дали дадени данни ще послужат за използваните метрики или не. Освен ако фирмата няма политика за продължително съхраняване на някои данни с цел възстановяването им, излишното събиране на данни е нежелателно.

Въпрос 3: Получавате ли полза или успявате ли да вникнете по-добре в нещата посредством метриката?

Вече беше отбелязано, че незрялостта на процесите за сигурност в ИТ индустрията не позволява сравнението на една фирма с друга. Това означава, че ползите трябва да се оценяват в рамките на собствената фирма. За това е достатъчно когато фирмата познава собствения си апетит и толеранс към риска. Важното е дали се получава полза от прилагането на метриките и дали тя си заслужава от гледна точка на влаганите разходи.

Въпрос 4: Какво искам да науча?

Отговорът на този въпрос е възлов за ефикасността на провежданите измервания. Специалистът трябва да си дава сметка за целите на организацията и да е способен да приотизира ценностите ѝ. По този начин се стеснява диапазонът от начини за придобиване на данни и информация и се спестяват време и усилия.

Въпрос 5: Кой, какво, кога, къде?

Вероятно 2/3 от тези въпроси могат да се отговорят с количествени метрики. По-долу има примерни въпроси.

Кой? Кои потребители имат достъп до чувствителна информация? Кой в организацията постоянно си избира слаби пароли?

Какво? Какво е съотношението на системите, които не са конфигурирани съобразно политиката за сигурност на фирмата? Обученията по сигурност ефективни ли са?

Кога? Колко често мениджмънтът преглежда стратегията за сигурност на компанията? Инцидентите в сигурността по-често ли се случват в рамките на работното време или извън него?

Къде? Кои организационни структури правят най-малко нарушения на правилата за сигурност за месец? Кой е най-честият източник на проучване срещу корпоративната мрежа?

Специалистите по информационна сигурност имат свои собствени въпросници. По много проблеми в края трябва да се отговори още на въпросите *Как и защо?* Отговорите на такива въпроси дават по-тълкувателни характеристики:

Как? Кои са най-скъпите ограничаващи фактори в текущия план за пачване? Кои потребители са най-добре ориентирани във фирмената стратегия за разкриване на електронна информация?

Как? Коя е първопричината за увеличаване на вирусните инфекции през последните 12 месеца? Икономическият спад причинил ли е по-висока податливост на вътрешни заплахи?

Използването на качествени и количествени метрики е решаващо за придобиване на пълна представа за заплахите или слабостите в информационното пространство на фирмата. Грешната интерпретация на резултатите или резултатите, придобити от грешна информация създават неточна представа за сигурността.

Освен това специалистът би могъл да изработи десетки количествени метрики, но те сами по себе си няма да са по-добри от това той да познава добре хората и средата в

например един център за данни (data center). Това е така, защото данните не дават информация за културните особености или за това дали няколко прилежни служители понасят тежестта на работата върху себе си. Това означава, че е възможно социалната среда да има решаващ ефект върху сигурността, а не само политиката на фирмата. Тези особености може да са обичайни или подразбиращи се за персонала, но специалистът не би могъл да ги разбере ако не зададе правилните въпроси. За тази цел е необходимо наблюдение и вслушване в хората.

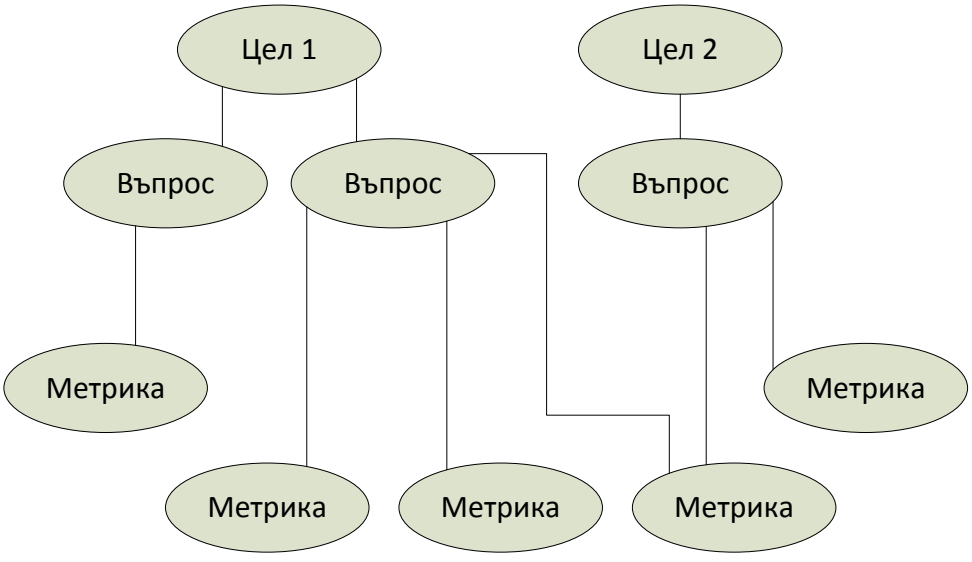
В този смисъл не е толкова от значение въпросът дали да използваме едни или други качествени или количествени метрики, а да ги направим емпирични, т.е. да провеждаме експерименти.

6.2. Методът „Цел-Въпрос-Метрика“ (ЦВМ)

ЦВМ е обикновен тристепенен процес за създаване на метрики в сигурността.

Първата стъпка от процеса е целеполагането: целите, които измерването трябва да постигне. След това целите се трансформират в още по-точни въпроси преди да се премине към измерване дали организацията е постигнала или постига целите си. Най-накрая на въпросите се отговаря чрез идентифициране и нагаждане на подходящите метрики и събиране на емпирични данни свързани с измерванията.

По-долу методът е представен графично. Трябва да се отбележи, че различни въпроси могат да водят до необходимостта от едни и същи метрики.



Фиг. 2

Използването на този метод носи със себе си три главни ползи. Първата е, че се следва последователен процес на създаване на метриката, започващ от целите, вместо от самите метрики. Втората полза е свързаността на дейностите по измерване с целите, което спомага да се поддържа фокусиране върху процеса. Третата полза е постигането на

уникални метрики, пригодни за съответната среда, съобразно уникалните цели на организацията и нейните особености.

По-долу трита елемента се разгледани по-подробно.

Целите

Добрите цели са специфични. Специфичните цели не довеждат до отворен край, както следните цели предполагат: „Подобряване на сигурността“ или „По-ефективно защитаване на чувствителната информация“. Конкретизирането спомага за лесно измерване на резултатите и съдейства за придържането към изработения план за действие. В същото време целеполагането трябва да прави целите гъвкави към промени.

Лимитирането на целите не означава, че специалистът трябва да ограничава способностите си да ги постигне. Целите трябва да са постижими, т.е. специалистът трябва да реши колко всеотдаен ще бъде, колко усилия ще трябва да положи и колко е толерансът му към риска от провал. При все това специалистът трябва да е изградил възможността да направи проверка до каква степен целите са постигнати.

От гледна точка на ефективността и възприемчивостта е полезно комплексните цели да бъдат разделени на множество подцели. При разписването на целта е подходящо да се следва следната схематичност:

Резултат – Елементи – Перспектива.

Резултатът е целта – какво желаем да постигнем. Например: Оценяване, разбиране, подобрение.

Елементите са границите и обектите (системи, процеси, характеристики), които засягат целта. Това могат да бъдат например уязвимостите, мрежите, потребителите и др.

Перспективата представлява гледната точка, според която целта ще бъде осъзната. Това може да е например гледната точка на атакуващите или на одиторите.

Един пример за целеполагането може да изглежда така:

„Целта на проекта е подобряване на изпълнението на политиката за сигурност и осведомеността за нея чрез увеличаване на познанието на потребителите за съдържанието на документите на фирмата по въпросите за сигурността от перспективата на мениджъра по сигурността.“

Задаване на въпроси

Въпросите са следващата стъпка на метода ЦВМ. Чрез тях оперативно се адресират свойствата на обектите. Специалистът по сигурността трябва да успява да задава правилните въпроси, водещи до изпълнението на целите и да идентифицира източниците на данни, които нямат пряка връзка с тях. Очевидни четири въпроса могат да се зададат при анализиране на компонентите на примерната цел по-горе:

1. Какво е моментното състояние на изпълнението на фирмената политика за сигурност?
2. Каква е моментната структура на фирмената политика за сигурност?
3. Дали служителите четат и разбират фирмената политика за сигурност?
4. Увеличава ли се изпълнението на политиката за сигурност?

Задаване на метрики

Със задаването на метриките се цели чрез тях да се отговори на въпросите преди това. Данните от ***първия*** на горните четири въпроси могат да засягат следните проблеми:

- Брой на документираните нарушения на политиката за сигурност през последните 12 месеца.
- Брой на действията, предприети срещу нарушенията на политиката за сигурност през последните 12 месеца.

Ако има по-малко предприети действия, отколкото нарушения, то тогава политиката не е била следвана във всяка една от ситуациите. Малкото информация или липсата на такава за това дали са правени въобще нарушения твърде вероятно може да означава, че фирмата няма поглед върху честотата на политиките, които се нарушават.

Вторият въпрос опитва да даде отговор за това какви са аспектите на политиките за инфраструктурата:

- Брой на документите, които описват политиката за фирмената сигурност.
- Формат(и) на документите за сигурност (хартиени носители, HTML, PDF и др.).
- Местоположение на документите за сигурност (система за управление на съдържанието, статична уеб страница, папки).
- Тип на механизмите за признаване валидността на политиките (съобщения по електронна поща до потребителите, друг вид електронно удостоверяване на достъпа, подпис върху физическо копие).
- Изминалото време от последния преглед на политиката за сигурност от мениджъра.

Както се вижда политиката на фирмата може да съществува едновременно в различни форми и източници. Знанието за структурата на тези източници подпомага специалиста в сигурността да изработи механизми за ефективно запознаване на служителите с фирмените политики в сигурността.

Третият въпрос разглежда поведението на служителите и поради техническата ограниченост на възможностите на специалиста да изследва съзнанието на всеки един от тях, се предпочита по-практичен метод. Според него измерването се извършва чрез наблюдение на поведението на хората и техните реакции, а получените резултати се сравняват с това, което специалистът е възприел за правилно. Разбира се, тук се намесва субективността, тъй като това, което смятаме за правилно и подходящо, може да не е достатъчно ефективно за поставените цели.

Подходящи метрики могат да бъдат:

- Съотношението на служителите с определени служебни задължения, показващо отговорността да следват фирмената политика за сигурност.
- Брой на дейностите за осведомяване на служителите за политиките за сигурност през последните 12 месеца.
- Съотношение на служителите, които през последните 12 месеца формално са получили знания за политиките за сигурност.

- Резултатите от допитвания до служителите, които задават въпроси за това до каква степен те са наясно с политиките за сигурност на фирмата и до каква степен тези политики са подходящи и полезни.

След установяване на настоящата начална позиция е подходящо да се изработят метрики, които да покажат дали се наблюдава развитие и подобрение на политиките за сигурност. Тук ***четвъртият въпрос*** може да доведе до създаването на следните метрики:

- Увеличаване на действията в политиките за сигурността над първоначалното ниво (изразено, или чрез определено число, или чрез процент).
- Увеличаване на знанието за фирмената политика за сигурност (брой на дейностите по запознаване, брой на потребителите, запознати с политиките).
- Увеличаване на ефективността на процесите за сигурност (увеличаване на броя на ревюта на политиките; намаляване на броя на документите или на местоположението на документите).
- Увеличаване на отговорите на потребителите за полезността на политиките.

Данните от тези метрики подпомагат специалиста по сигурността да вземе решения, които са били подценени в началото на проекта. Те дават яснота до каква степен проектът изпълнява целите си и съдействат за правенето на заключения за необходимостта от промяна на дейностите.

Методът ЦВМ се прилага за конкретна среда и с всяка нова информация за нея той може да бъде променян периодически. Този метод има силна практическа стойност, тъй като може да приеме табличен вид във формата на образец (темплейт).

Този метод не отговаря на въпроса какво трябва да се постигне по отношение на сигурността. Казано по друг начин – ЦВМ не създава идеи, а подпомага организацията на специалиста по сигурността.

V. ЗАКЛЮЧЕНИЕ

Представените особености на различни класификации на метриките за информационна сигурност, както и силните и слабите страни на по-известните метрики, съдействат за разбирането за процеса на управление на информационната сигурност.

Най-общо метриките могат да се разделят на мениджърски, операционни и технически, като те са неразривно свързани помежду си.

Ефективните метрики в областта на сигурността са тези, които са пригодени и изработени за целите на конкретната организация, без значение дали са количествени или качествени.

Главният специалист по информационната сигурност трябва да има подходящи знания и умения за изработване на качествени анализи, доклади и оценки на сигурността в една организация, за всеки от нейните йерархични звена. Той трябва да е в състояние да преценява правилно фирмените цели и да ги приоритизира съобразно ограничените ресурси. Това са задължителни компоненти за ефективно управление на процеса на информационна сигурност.

ЛИТЕРАТУРА

Oxford American Dictionary, Oxford: Oxford University Press, 2013, http://www.oxforddictionaries.com/definition/english/metric?q=metric

The CIS Security Metrics, Center for Internet Security, November 2010, https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf

Lance Hayden, *IT Security Metrics A Practical Framework for Measuring Security & Protecting Data*, Mc Graw Hil, 2010, http://labkom.stikom.edu/download/ebook/0071713409Security.pdf

Anni Sademies, *Process Approach to Information Security Metrics in Finnish Industry and State Institutions*, Otamedia Oy, Espoo 2004, http://www.vtt.fi/inf/pdf/publications/2004/P544.pdf

Marianne Swanson & Co, *Security Metrics Guide for Information Technology Systems*, Gaithersburg: National Institute of Standards and Technology, MD 20899, July 2003, http://www.rootsecure.net/content/downloads/pdf/nist_security_metrics_guide.pdf