IT4Sec Reports 146
http://dx.doi.org/10.11610/it4sec.0146

Модел за оценяване на зрелостта на способностите за киберсигурност на базата на балансирана карта от показатели за ефективност

Венелин Георгиев

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

София, септември 2022

Венелин Георгиев, Модел за оценяване на зрелостта на способностите за киберсигурност на базата на балансирана карта от показатели за ефективност**,** *IT4Sec Reports 146* (септември 2022), http://dx.doi.org/10.11610/it4sec.0146

IT4Sec Reports 146 „Модел за оценяване на зрелостта на способностите за киберсигурност на базата на балансирана карта от показатели за ефективност" Измерването на зрелостта на способностите за киберсигурност е ключов елемент от цялостната концепция за изграждане и поддържане на сигурност в киберпространството. В доклада се представят резултатите от създаването на модел за оценяване на зрелостта на способностите за киберсигурност като съчетание от предимствата на балансираната карта от показатели за ефективност и бенчмарк модел. Разработеният модел притежава силата на теоретичната обоснованост и практическата приложимост.

Ключови думи: киберсигурност, способности, ефективност, бенчмарк, зрялост, модел

IT4SecReports 146 "Cyber Security Capabilities Maturity Model Based on a Balanced Scorecard" Measuring the maturity of cybersecurity capabilities is a key element of the overall concept of building and maintaining security in cyberspace. The report presents the results of the creation of a model for assessing the maturity of cybersecurity capabilities as a combination of the advantages of the balanced scorecard and benchmark model. The developed model has the strength of theoretical validity and practical applicability.

Keywords: cybersecurity, capabilities, efficiency, benchmark, maturity, model

Редакционен съвет

Председател: акад. Кирил Боянов
Редактори: д-р Стоян Аврамов, проф. Генадий Агре, доц. Кирил Алексиев, проф. Даниела Борисова, проф. Венелин Георгиев, проф. Величка Милина, доц. Златогор Минчев, доц. Георги Павлов, проф. Тодор Тагарев, доц. Велизар Шаламанов
Отговорен редактор: Наталия Иванова

© Венелин Георгиев, 2022 г.

ISSN 1314-2119

ВЪВЕДЕНИЕ

Изследването, резултатите от което се представят в доклада се основава на три основни въпроса. Първият се отнася до това необходимо ли е да бъде измервана зрелостта на способностите за киберсигурност. Положителният отговор се аргументира с естествената човешка реакция да измерва всяка извършвана дейност. Резултатите от измерването се използват за да бъде установена степента, до която е постигната предварително поставена цел, в случая целта е под формата на зададено ниво на зрялост на способностите за киберсигурност. Вторият въпрос се интересува от това защо точно способностите за киберсигурност трябва да бъдат измервани по отношение на тяхната зрялост. Аргументите този път са в посока към значимостта и мащабите на киберзаплахите, срещу които се използват този тип способности. Обикновено щетите от кибератаките на годишна база се измерват в стотици милиарди американски долари, като при това щетите са не само за големите компании и публичните институции, но и за отделните потребители на услуги в киберпространството. Третият въпрос реферира към това по какъв начин, с помощта на какви инструменти да бъде измервана зрелостта на способностите за киберсигурност. В проведеното изследване се комбинират два универсални мениджърски инструменти каквито са балансираната карта по показатели за ефективност и модел за бенчмаркинг Балансираната карта дава възможност за определяне на областите, в които да бъде измервана зрелостта на способности. Моделът за бенчмаркинг от своя страна позволява да бъдат структурирани нивата на зрялост, изискващите се състояния и техните целеви стойности. Комбинацията от двата мениджърски инструмента прави възможно зрелостта на способностите за киберсигурност да бъде измерена по един достатъчно системен и научно обоснован начин, който освен всичко друго е обективен и лесно приложим в практиката.

БАЛАНСИРАНА КАРТА ОТ ПОКАЗАТЕЛИ ЗА ЕФЕКТИВНОСТ

Балансираните карти от показатели за ефективност са въведени в практиката от професорите на Харвардския университет Робърт Каплан и Дейвид Нортън.[1] Идеята на балансираните карти е да запази използването на финансови метрики при измерване на резултатите, но към тях да се добавят и друг тип метрики, с помощта на които да се създадат условия за по-пълното и по-правилното измерване на резултатите от човешката дейност. Тези допълнителни гледни точки се постигат за сметка на използването на нефинансови метрики, които придават числови стойности на външни индикатори като очаквания на потребителите, а също така осигуряват по-дълбоко вникване в мотивацията на персонала на организацията и в нейните вътрешни процеси.

Балансираният характер на картите е за сметка на разделяне на използваните метрики в четири групи: финансови, потребители, вътрешни процеси, обучение (виж фиг. 1). Авторите на балансираните карти смятат, че тези четири области за измервания, взети заедно, могат да създадат достатъчно точен образ на организацията и на получаваните резултати от организационните дейности. Метриките от четирите направления измерват дадения обект спрямо типичните и конкретизирани отправни точки, каквито са мисията, визията, стратегията и ценностите за организацията.[2]

Балансираната карта от показатели за ефективност представлява рамка, в която всеки потребител и всяка организация е в състояние да избира:

---

[1] Robert Kaplan and David Norton, *The Balanced Scorecard: Translating Strategy Into Action* (Boston: Harvard Business School Press, 1996).

[2] Robert Kaplan and David Norton, “Putting Balanced Scorecard to Work,” *Harvard Business Review* (September-October 1993), https://hbr.org/1993/09/putting-the-balancedscorecard-to-work.

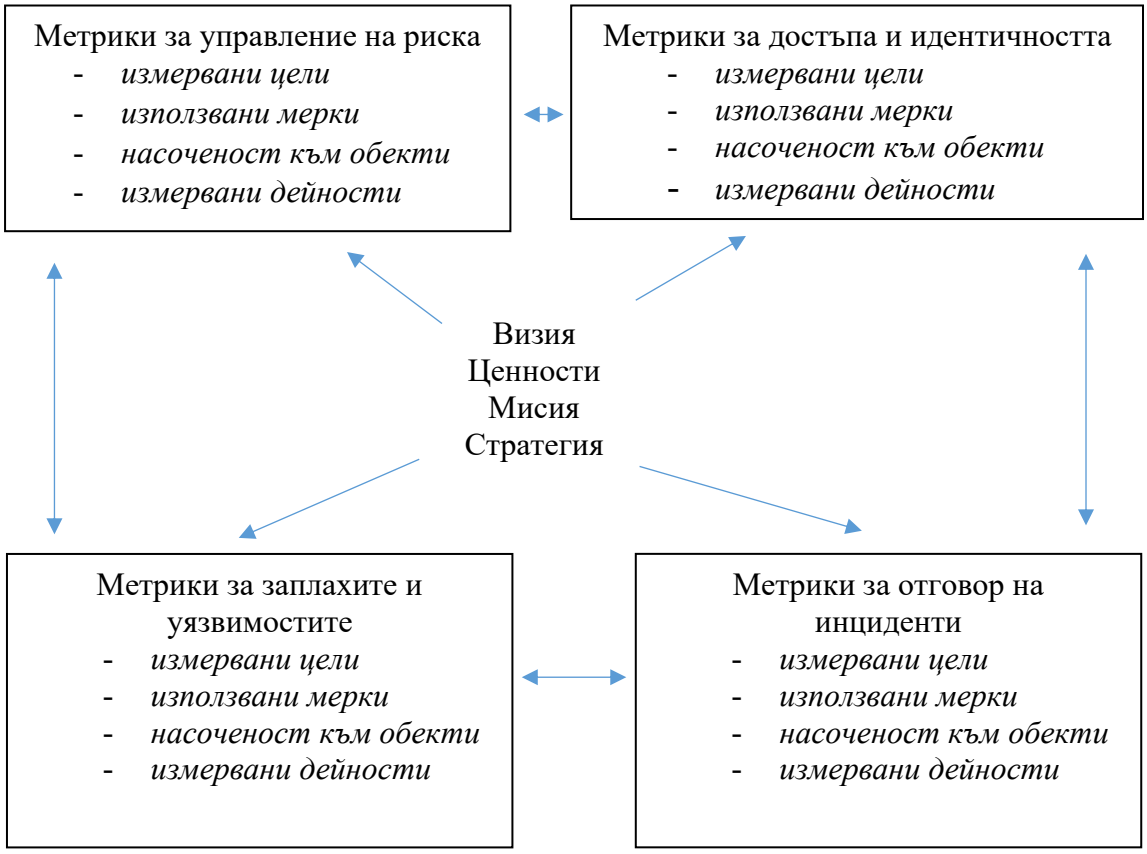
- в какъв аспект от дейността на организацията да бъде разработена и използвана картата;
- какви да бъдат четирите области, които да формират направленията за измерване;
- какви конкретни метрики да бъдат използвани предвид на това същите да отговарят на спецификата на организацията по най-добрия начин и да се вписват в организационната култура и стратегия.

Фиг. 1. Схема на класическата балансирана карта от показатели за ефективност

Горните характеристики на балансираната карта от показатели за ефективност дават свобода при нейното използване и на тази база е разработена балансирана карта от показатели за ефективност на способностите за киберсигурност[3]. Както се вижда от фиг. 2, направленията, в които се измерват резултатите от киберсигурността включват управление на риска, достъпа до информационните активи и идентичността на потребителя, заплахите и уязвимостите за информационните активи, способност за реакция и отговор при инцидент с киберсигурността. Във всяка от четирите области се дефинират целите, които организацията преследва, измерваните дейности и обекти, както и метриките, с помощта на които се представят оперативните и целевите резултати. Както и при класическия вариант на балансираната карта, измерванията в четирите области на киберсигурността се адресират към мисията, визията, стратегията и ценностите на организацията. Характерно за прилагане на балансираната карта от показатели за ефективност в сферата на киберсигурността е, че измерваните резултати за ефективността на метриките за киберсигурност се отнасят и съпоставят с начина, по който те допринасят за постигане на целите на стратегическия мениджмънт на организацията в четирите области на класическата балансирана карта, а

[3] Венелин Георгиев, *Сценарийно планиране на способности за киберсигурност* (София: Авангард, 2021).

именно финансови резултати, вътрешни процеси, удовлетвореност на потребителите, обучение.



Фиг. 2. Модел на балансирана карта от показатели за ефективност на мерките за киберсигурност в организацията

ПРИНЦИПЕН МОДЕЛ ЗА ОЦЕНЯВАНЕ НА ЗРЕЛОСТТА НА ДАДЕН ОБЕКТ

Способностите за киберсигурност на организацията представляват динамичен обект, чието управление изисква възможности за измерване на нивото на тяхната зрялост и сравняване на оперативните стойности с предварително определени целеви стойности (най-често в националните стратегии за киберсигурност). За нуждите на измерването нивото на зрялост на способностите за киберсигурност е необходим модел, който да бъде адекватен на обекта, чийто способности се измерват.

Инцидентите с киберсигурността на организациите от всякакъв мащаб и всякакъв вид дейност показват и доказват необходимостта от изграждане на способности за поддържане на този вид специфична и жизнено важна сигурност. Проследяването на тенденциите показва нарастване на броя и интензивността на киберзаплахите, които създават едни от най-сериозните оперативни рискове, пред които се изправя съвременното общество. При тези условия организациите се нуждаят от познаване и прилагане на достатъчно ефективен модел за измерване и оценяване на зрелостта на способностите си за киберсигурност, на базата на който да бъдат разработвани и актуализирани адекватни програми и процедури.

В общия случай един такъв модел се фокусира върху определяне и изпълнение на дейностите, практиките и процедурите в областта на киберсигурността, свързани с

информационните и оперативните технологии, средства и средата, в която организацията функционира. Моделът представлява съвкупност от характеристики, инструменти и метрики, които показват както текущото състояние, така и напредъка при създаване на способности в различни области на киберсигурността[4]. Друго предимство на модела е възможността, която предоставя на организацията за измерване и оценяване на процесите и практиките на базата на ясни показатели по метода на бенчмаркинг. В тази посока моделът допуска използване както на добри практики в областта на сигурността, така и на съществуващи стандарти и изисквания на регулаторни институции на международно, национално и локално ниво. Използването на модела е итеративен процес, т.е. с помощта на модела може да се оцени текущото състояние на способностите за сигурност, като при повторна оценка може да се установи напредъка в различните области на сигурността. В архитектурно отношение моделът включва области от полето на сигурността; нива, организирани в рамката на съответната скала; метрики, с помощта на които се установява прехода от едно ниво към друго (виж фиг. 3). За да бъде достатъчно ефективно и резултатно използването на модела следва да се събират и анализират емпирични данни за всяка от изследваните области на сигурността и за всяка от отчитаните дейности.

Прилагането на модел за оценяване на зрелостта на способностите за сигурност дава възможност за:

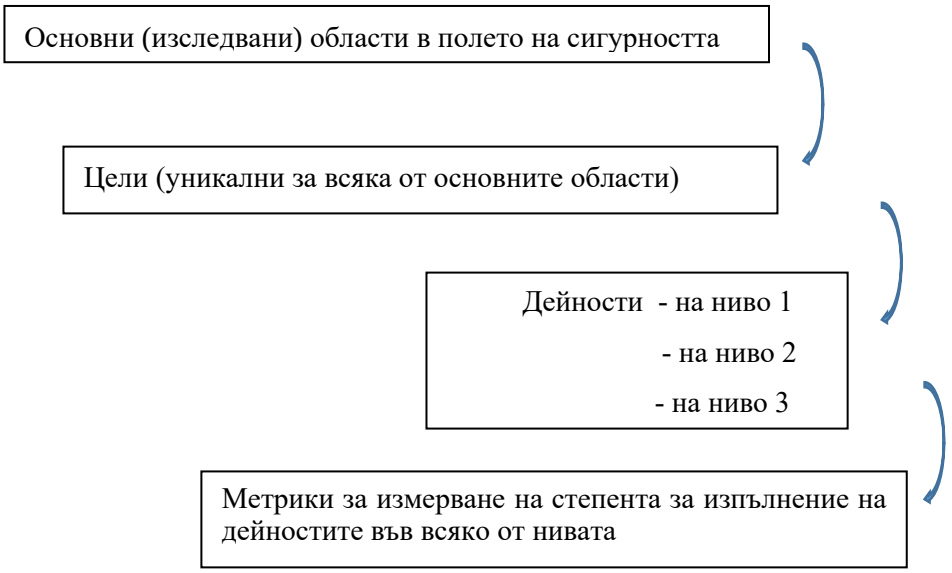
- повишаване на равнището на организационните способности за сигурност;

- достатъчно ефективно и непрекъснато оценяване на организационните способности за сигурност и сравняването им с познати добри практики;

- споделяне на знание и добри практики между организациите като инструмент за подобряване на способностите им за сигурност;

- приоритизиране на дейностите и инвестициите в интерес на сигурността.

Архитектура на модела за оценяване на зрелостта на способностите за сигурност:



Фиг. 3. Архитектурен модел за оценяване на зрелостта на способности за сигурност

[4] George Sharkov, "Assessing the Maturity of National Cybersecurity and Resilience," *Connections: The Quarterly Journal* 19, no. 4 (2020): 5-24.

Схематично, използването на един принципен модел за оценяване на зрелостта на способностите за сигурност може да бъде представено по следния начин (виж фиг. 4)[5]:

В обобщен вид, при прилагане на модела организацията извършва оценка на текущото ниво на своите способности за сигурност, анализира получените резултати и идентифицира липсващите способности (capability gaps), приоритизира липсващите способности и планира дейностите по тяхното изграждане, изпълнява разработения план и следи за измененията в нивото на способности за сигурност, които се използват при следващия цикъл от прилагане на модела. Като аргументи за необходимостта от повторно прилагане на модела могат да бъдат посочени промяната в средата, в която оперира организацията, промяна в заплахите и рисковете за сигурността, промяна в целите и стратегиите на организацията и т.н.

Фиг. 4. Схема за прилагане на модел за оценяване на зрелостта на способностите за сигурност

МОДЕЛ ЗА ОЦЕНЯВАНЕ НА ЗРЕЛОСТТА НА СПОСОБНОСТИТЕ ЗА КИБЕРСИГУРНОСТ НА БАЗАТА НА БАЛАНСИРАНА КАРТА ОТ ПОКАЗАТЕЛИ ЗА ЕФЕКТИВНОСТ

Както беше отбелязано, създаването на модел за оценяване на зрелостта на способностите за киберсигурност използва описаните по-горе два мениджърски инструменти. От балансираната карта се взимат областите от полето на киберсигурността, за които се извършва оценяването на зрелостта на способностите. В конкретния случай това са областите за управление на риска за информационните активи, управление на достъпа до информационните активи и идентичността на потребителя, заплахите и уязвимостите за информационните активи, способностите за реакция и отговор при инцидент с

[5] Gregory White, “The Community Cyber Security Maturity Model,” *2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07)*, *Waikoloa, Big Island, HI, USA*, 2007.

киберсигурността. С тези области се захранва архитектурния модел от фигура 3 като за тях се формулират целите, дейностите от съответните нива и метриките, с помощта на които се измерва степента за постигането на тези цели.

За по-голяма яснота, по-долу е направено описание на съдържанието на модела за една от избраните области:

- изследвана област в полето на киберсигурността: управление на риска за информационните активи;
- цел: създаване на условия за достатъчно ефективно идентифициране, анализира, оценяване, преценяване и противодействие срещу рисковете за информационните активи;
- дейности на ниво 1:
- организацията не прилага системен процес за управление на риска, а обръща внимание на риска само при възникване на съществени инциденти със сигурността на информационните активи;
- организацията не събира информация и не води регистър на рисковете за информационните активи;
- организацията няма дефинирано ниво на апетит към риска и не разграничава приемливите от неприемливите рискове.
- дейности на ниво 2:
  - организацията разполага с методика за управление на риска за информационните активи и прилага системен процес в тази област;
  - в организацията се води регистър на рисковете за информационните активи, който периодично се обновява;
  - в организацията е зададено нивото на приемлив риск, на базата на което се разработват стратегии за противодействие срещу неприемливите рискове;
- дейности на ниво 3:
  - в организацията има изграден процес за периодичен преглед, актуализиране и развитие на документите в областта на управлението на риска за информационните активи;
  - воденият в организацията регистър на рисковете е достъпен за всички участници в процеса по управление на риска, като от него се предоставя при нужда информация за външни потребители;
  - организацията периодично преглежда прилаганите стратегии за противодействие срещу неприемливите искове и оценява тяхната ефективност.
- метрики за измерване степента за изпълнение на дейностите от съответните нива: наличие на методика за оценка на риска; наличие на регистър на рисковете за информационните активи; количествени и качествени параметри за апетита към риска; средно време за актуализиране на документите по управление на риска; размер на ресурсите, изразходвани в процеса за управление на риска и др.

По същия начин могат се дефинират целите, дейностите и метриките за останалите три област от модела за оценяване на зрелостта на способностите за киберсигурност на базата на балансираната карта от показатели за ефективност.

ЗАКЛЮЧЕНИЕ

Комбинирането на два инструмента от мениджърската теория и практика, каквито са балансираната карта от показатели за ефективност и модел за бенчмарк, при създаване на модел за оценяване на зрелостта на способностите за киберсигурност се оказва добро

решение. Аргументираният избор на области от полето на киберсигурността, които да бъдат отчитани в изследването и подходящото определяне на нивата на зрялост, съответните дейности и метриките за измерване на тяхното изпълнение придават на създадения модел теоретична обоснованост и практическа приложимост. Създаденият модел за оценяване на зрелостта на способностите за киберсигурност притежава нужните характеристики за да бъде причислен към семейството от подобни модели и единственото, което остава е този модел да намери приложение в практиката на бизнес организациите и на публичните институции.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] Robert Kaplan and David Norton, *The Balanced Scorecard: Translating Strategy Into Action* (Boston: Harvard Business School Press, 1996).

[2] Robert Kaplan and David Norton, “Putting Balanced Scorecard to Work,” *Harvard Business Review* (September-October 1993), https://hbr.org/1993/09/putting-the-balancedscorecard-to-work.

[3] Венелин Георгиев, *Сценарийно планиране на способности за киберсигурност* (София: Авангард, 2021).

[4] George Sharkov, “Assessing the Maturity of National Cybersecurity and Resilience,” *Connections: The Quarterly Journal* 19, no. 4 (2020): 5-24.

[5] ENISA, “CSIRT Maturity - Self-assessment Tool,” 2022, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey.

[6] Gregory White, “The Community Cyber Security Maturity Model,” *2007 40th Annual Hawaii International Conference on System Sciences (HICSS’07)*, *Waikoloa, Big Island, HI, USA*, 2007.