Измерване на равнището от способности за киберсигурност на организация

професор д-р Венелин Георгиев

Резюме: Проследяването на тенденциите демонстрира 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 способностите си за киберсигурност, на базата на който да бъдат разработвани и актуализирани адекватни планове, програми и процедури. В доклада се представят резултатите от адаптираното приложение на модела Cyber capability maturity model (C2M2) при структуриране на подход за оценяване на способностите за киберсигурност. Подходът включва структуриране на полето на киберсигурността на отделни области, формулиране на специфични за всяка от областите цели и дейности за киберсигурност, създаване на скала и метрики за измерване на степента за постигане на поставените цели.

Ключови думи: киберсигурност, киберзаплахи, риск, способности, метрики, измерване.

Abstract: Trend tracking demonstrates an increase in the number and intensity of cyber threats that create one of the most serious operational risks for modern society. Under these circumstances, organizations need to know and implement a sufficiently efficient model for measuring and evaluating their cyber security capabilities, based on which to develop and update adequate plans, programs and procedures. The report presents the results of the adapted application of the Cyber capability maturity model (C2M2) in structuring an approach to assessing cybersecurity capabilities. The approach involves structuring the cybersecurity field of individual areas, formulating cybersecurity-specific targets for each area, setting up a scale and metrics to measure the extent to which the targets are being met.

Key words: cyber security, cyber threats, cyber risk, capabilities, metrics, evaluation.

Общо описание на модела за измерване на равнището на организационните способности за киберсигурност

Инцидентите с киберсигурността на организациите показват и доказват необходимостта от изграждане на способности за поддържане на този вид специфична и жизнено важна сигурност. От друга страна, 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 адекватен и ефективен модел за измерване и оценяване на способностите си за киберсигурност, на базата на който да бъдат разработвани и актуализирани адекватни политики, програми и процедури за сигурност.

Пример за подобен модел е Cyber capability maturity model (C2M2), който се фокусира върху определяне и изпълнение на дейностите, практиките и процедурите в областта на киберсигурността, свързани с информационните и оперативните технологии, както 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. 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 бенчмаркинга. В тази посока моделът допуска използване както на добри практики в областта на киберсигурността, така и на съществуващи стандарти и изисквания на регулаторни институции. Използването на модела е итеративен процес, т.е. с помощта на модела може да се оцени текущото състояние на способностите за киберсигурност, като при повторна оценка може да се установи напредъка в различните области на киберсигурността. В архитектурно отношение моделът включва нива, организирани в рамката на съответната скала и метрики, с помощта на които се установява прехода от едно ниво към друго. За да бъде достатъчно ефективно и резултат-

но използването на модела следва да се събират и анализират емпирични данни за всяка от изследваните области на киберсигурността. Правилното използване на модела се нуждае от намиране на отговори на следните въпроси:

– откъде и кога да започне изследването и оценяването на способностите на организацията за киберсигурност;

– по какъв начин да бъде използван конкретният опит на организацията;

– какъв да бъде общият език за комуникиране между всички участници в процеса на използване на модела;

– по какъв начин да бъдат направени подобренията, водещи от текущото към желаното (целевото) ниво на способности за киберсигурност;

– на каква база да бъдат приоритизирани планираните дейности и инвестиции за развитие на способностите за киберсигурност.

Прилагането на модела C2M2 дава възможност за:

– повишаване на равнището на организационните способности за киберсигурност;

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

– споделяне на знание и добри практики между организациите като инструмент за подобряване на способностите им за киберсигурност;

– приоритизиране на дейностите и инвестициите в интерес на киберсигурността.[1]

Разглежданият модел се базира на методика за самооценяване, с помощта на която организацията измерва, оценява и подобрява своята програма за киберсигурност. Успоредно с това въпросният модел може да се използва в процеса за разработване на нова програма за киберсигурност. Приложението C2M2 води до създаване по-скоро на описателни препоръки, а не толкова на задължителни изисквания. По отношение на приложимостта му, моделът може да бъде адаптиран за нуждите на организации от всякакъв мащаб, икономически сектор, тип на дейността и структура.

C2M2 съчетава съвкупност от характеристики и метрики, които описват способностите за киберсигурност и тяхното развитие в предварително определени области. В съдържанието на модела са включени също така добри практики и стандарти в областта на сигурността на информационните системи и мрежи. По този начин моделът създава възможност за бенчмаркинг и оценяване на текущото ниво на способности за киберсигурност на организацията, както и за приоритизиране на действията и инвестициите за тяхното развитие.

За измерване на текущото състояние и прогреса при развитие на способностите за киберсигурност, в модела се използва скала с различни нива (от 0 до 3), показващи зрелостта на организационните способности за киберсигурност. За всяко от нивата се използват подходящи показатели и метрики, които го описват. Констатирането на изпълнение на даден показател се приема за доказателство за това, че организацията притежава съответните способности за киберсигурност. Възможността за измерване на състоянието на организационните способности за киберсигурност с помощта на описаната скала прави възможно:

– определяне на текущото състояние на способностите за киберсигурност;

– определяне на желаното целево или бъдещо състояние на способностите за киберсигурност;

– определяне на т.нар. липсващи способности (capability gaps), които следва да бъдат изградени за да се премине от текущото към бъдещото състояние на способностите за киберсигурност.

Структура на модела за измерване на равнището от способности за киберсигурност на организацията

На ниво организация, моделът C2M2 се адаптира и прилага на базата на възприети стандарти и разработени програми и процедури за киберсигурност. Моделът осигурява достатъчно гъвкави и адаптивни указания на ръководството на организацията към професионалистите и потребителите по отношение на киберсигурността. В общия случай, в съдържанието на модела се включват десет основни области, покриващи цялостната дейност в областта на киберсигурността.[2] Всяка от тези области включва логически групирани практики от сферата на киберсигурността. Дейностите във всяка от областите са групиране около съответни цели, които организацията се опитва да постигне. Измерването на степента на постигане на всяка от целите става с помощта на подходящи метрики за всяко от нивата на скалата.

Основни области в полето на киберсигурността (10)
Цели (уникални за всяка от основните области)
Дейности – на ниво 0, метрики
– на ниво 1, метрики
– на ниво 2, метрики
– на ниво 3, метрики

Фиг. 1. Структура на модела за оценяване на организационните способности за киберсигурност

Всяка от десетте общи области от дейности в сферата на киберсигурността се описва със следните компоненти: обхват или предназначение, обяснителни бележки, цели, дейности, метрики. Дейностите във всяка от общите области са обединени около една или няколко цели. Като пример, в областта на управление на риска за киберсигурността дейностите могат да бъдат обединени около три цели, включващи: създаване на стратегия за управление на риска за киберсигурността; управляване на риска за киберсигурността; мениджмънт на изпълняваните дейности. Структурата на модела C2M2 е представена на фигура 1.

Кратко описание на съдържанието на десетте общи области от сферата на киберсигурността, използвани в съдържанието на модела C2M2, може да бъде направено по следния начин:

– управление на риска за киберсигурността,

което включва създаване, прилагане и поддържане на програма за управление на риска с цел идентифициране, анализиране и снижаване на заплахите и рисковете за киберсигурността на организацията;

– управление на средствата, промените и конфигурацията, което се изразява в управление на информационните и оперативните средства на организацията, в това число хардуер и софтуер по начин, кореспондиращ с управлението на риска за киберсигурността;

– управление на достъпа и идентичността, което на практика представлява управление на идентичности, които да гарантират логическия и физическия достъп до информационните системи и мрежи на организацията, както и контролиране на достъпа по начин, отговарящ на изискванията за управление на риска за киберсигурността;

– управление на заплахите и уязвимостите, разбирано като разработване и прилагане на планове, процедури и технологии за откриване, идентифициране, анализиране, снижаване и отговор на заплахи и уязвимости в сферата на киберсигурността, съизмерими или пропорционални на целите на организацията;

– следене на текущото състояние на киберсигурността, което се изразява в организиране и провеждане на дейности за събиране, анализиране, представяне и използване на информация, отнасяща се до киберсигурността на организацията;

– споделяне на информация и комуникиране, което на практика включва изграждане и поддържане на отношения с вътрешни и външни субекти с цел събиране и осигуряване на информация за киберсигурността, включваща заплахи, уязвимости, снижаване на риска, повишаване на устойчивостта по начин, пропорционален на целите на организациите;

– отговор на инциденти и поддържане на непрекъснатостта на бизнеса чрез разработване и изпълнение на планове и процедури за откриване, анализиране и противодействие срещу инциденти с киберсигурността, а също така и поддържане на непрекъсваемостта на бизнеса чрез действия в полза на киберсигурността на организацията;

– управление на веригите за доставка и на външните зависимости, изразяващо се в създаване и прилагане на инструменти за контролиране на риска, свързан с активите и услугите, които са зависими от външни за организацията субекти;

– управление на персонала чрез разработване и изпълнение на планове и процедури за изграждане на организационна култура за киберсигурност, осигуряване на достатъчно ниво на компетентност от страна на персонала;

– управление на програмата за киберсигурност, което включва разработване и изпълнение на подобна програма в организацията, съдържаща необходимите дейности за изграждане и поддържане на целево ниво на киберсигурност по начин ,който прави целите пред киберсигурността част от общите цели на организацията.[3]

За всяка от основните области, формиращи полето на киберсигурността на организацията се формулират цели, за постигането на които се задават и конкретни дейности. Измерването на степента на изпълнение на дейностите става с помощта на скала, включваща четири степени или нива, съответно от 0 до 3. Тези нива се прилагат при оценяване изпълнението на дейностите и постигането на целите за всяка от основните области на киберсигурност.

Метриките, прилагани в рамките на всяко от нивата се използват в две направления: за измерване на състоянието на способностите за киберсигурност на организацията и за оценяване на ефективността на самия подход за изграждане на способности за киберсигурност. Правилното прилагане на модела C2M2 изисква разбиране на следните четири характеристики на нивата от скалата за измерване:

– Нивата се прилагат независимо за всяка от общите области на киберсигурността. Като резултат от това е възможно за една и съща организация да съществуват различни нива при отделните общи области на киберсигурността.

– Нивата са кумулативни, което означава че за да бъде в съответното състояние или ниво, организацията трябва да изпълнява всички изисквания за това ниво, а също така и за всички предходни. Като пример, за да бъде организацията в дадена обща област на киберсигурността на ниво 2 тя трябва да е изпълнила изискванията, включени в същата област за нива 1 и 2.

– Определянето на желаното или целевото ниво за всяка от общите области на киберсигурността е подходяща стратегия при управление изпълнението на програмата за киберсигурност. Определянето на целевите нива за общите области изисква предварително запознаване с тяхното съдържание, определяне на несъответствията между текущите и желаните (бъдещите) способности и фокусиране на усилията върху преодоляването на тези несъответствия.

– Определянето на целевите нива на способности за всяка от общите области на киберсигурност следва да става в рамките на определените общи цели за бизнеса и на базата на стратегията за киберсигурност на организацията. Стремежът към постигане на максимални нива на способностите във всяка от общите области на киберсигурността не винаги е оправдан, рационален и възможен. При определяне на целевите нива следва да се отчитат разходите, за сметка на които се получават ползите под формата на способности за киберсигурност.[4]

Изграждането и поддържането на адекватни способности за киберсигурност се превръща в ключов въпрос на сигурността предвид на значимостта и интензивността на заплахите за сигурността на съвременните компютърни системи, мрежи и на обработваната и съхраняваната в тях информация. Контролирането на нивото на създаваните способности за киберсигурност е свързано с възможностите за тяхното измерване като текущо състояние и като съответствие на зададените целеви стойности. Разгледаният в доклада модел за определяне на нивото на способностите за киберсигурност се характеризира със своята креативност, намираща израз във възможностите от страна на изследователите да подбират подходящи за конкретното изследва-

не области, цели, дейности и метрики за измерване на текущото и целевото ниво на способностите за киберсигурност. Получаваните резултати могат да бъдат сравнявани със съществуващи стандарти или добри практики, като по този начин да се постига увереност в зрелостта на организацията по отношение на усилията за гарантиране на нейната киберсигурност и готовност за противодействие срещу киберзаплахите под формата на конкретни кибератаки.

---

[1] Georgiev, V. Planirane za sposobnosti za kibersigurnost na bazata na stsenarii. Sofia: Avangard, 2016.
[2] Christipher J. Cybersecuriy Capability Maturity Model. Department of Energy. Department of Homeland Security, 2014.
[3] Ibidem.
[4] Georgiev, V. Planirane za sposobnosti …