IT4Sec Reports 141
http://dx.doi.org/10.11610/it4sec.0141

Концептуален модел за устойчивост в сигурността

Венелин Георгиев

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

София, септември 2021

Венелин Георгиев, Концептуален модел за устойчивост в сигурността**,** *IT4Sec Reports 141* (септември 2021), http://dx.doi.org/10.11610/it4sec.0141

IT4Sec Reports 141 „Концептуален модел за устойчивост в сигурността“ Възприемането на тезата за отсъствие на пълна сигурност, която се доказва от многобройните примери за инциденти със сигурността, насочва вниманието на изследователите и практиците към възможностите за изграждане на устойчиви системи в сигурността. Характерно за подобен тип системи е възможността за запазване на оперативната функционалност на ключови процеси и на поддържащите ги активи в условия на смутена среда. В доклада се представят резултатите от изследване, насочено към създаване на концептуален модел на система за устойчивост в сигурността, който е теоретично аргументиран и с висока степен на практическа приложимост.

Ключови думи: сигурност, устойчивост, активи, технологии, риск

IT4Sec Reports 141 Venelin Georgiev, “A Conceptual Model for Resilience in the field of Secuirty” It is already understood that security cannot be guaranteed. Numerous examples of security incidents prove that, and direct both researchers and practioners to explore the opportunities for development of security systems that are resilient. A common feature of the resilient systems is that they preserve the functionality of core processes and their supporting assets under perturbations. This report presents the results of a study aiming to deliver a conceptual model of the system for resilience in the field of security, that is supported by theoretical arguments and applicable in practice.

Keywords: security, resilience, assets, technologies, risk

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

© професор д-р Венелин Георгиев, 2021 г.

ISSN 1314-5614

ВЪВЕДЕНИЕ

Като свойство на обектите и системите, устойчивостта е представена и видима по най-добър начин в природата. Дърветата са създадени да понасят, но да не се пречупват от тежестта на натрупвания върху клоните им сняг или под напора на бурни ветрове. Човешкото тяло е с възможности за пречистване на кръвта, възстановяване на клетки и отговор на атаки от страна на бактерии и вируси. Сърцевината на устойчивостта, и в частност на устойчивостта в сигурността, е в подготовката за отговор на въздействия от страна на средата, но не чрез реакция (реактивно), а по-скоро чрез адаптиране и приспособяване (адаптивно).

Във времето терминът „устойчивост“ се дефинира и интерпретира по различни начини в зависимост от контекста, в рамките на който е бил използван. Като примерна дефиниция за устойчивост може да бъде посочена способност на организацията да се подготви и планира за приемане, възстановяване и успешно адаптиране към нежелани събития. Друго определение казва, че устойчивостта представлява способност на организацията да се подготви за и адаптира към променящи се условия, както и бързо да се възстановява след въздействия. Онова, което обединява горните две определения за термина устойчивост са характеристиките:

- *адаптиране*, изразяващо се в промяна в мениджърския подход и в стратегията за отговор преди настъпване на разрушителното събитие или бъдещата заплаха на базата на поуките от практиката от предходни инциденти;
- *подготовка*, намираща израз в предвиждане и планиране срещу потенциални заплахи и стресори, както и идентифициране и контролиране на критичните функции на системите, изложени на риск;
- *издръжливост* или способност за поддържане на работоспособност без съществени ограничения и загуба на функционалност при възникване на инцидент;
- *възстановяване*, изразяващо се в способност за завръщане към първоначалния пълен обем на дейностите и функционалностите след отстраняване на инцидента.

Един от аспектите, в рамките на който могат да се водят дискусии по проблемите на устойчивостта като характеристика на системата за сигурност е съпоставянето на устойчивостта и сигурността. Образно казано, предназначението на сигурността е да държи „злосторниците“ вън от защитаваните обекти, системи, приложения, периметри и т.н. Като пример, една държава решава да построи стена, която да спира нежеланите посетители. Тази стена може да бъде много висока, снабдена с различни технически и физически средства, които да затрудняват достъпа, но остава въпросът дали сама по себе си стената ще бъде достатъчна за постигане на целта. Пример, който е актуален към настоящия момент е техническото съоръжение (оградата) на южната граница на България. В рамките на същия сценарий, възможна алтернатива е построяването на няколко стени като тази алтернатива се представя в литературата с термина „защита в дълбочина“. За съжаление и двете алтернативи не гарантират, че ще спрат достъпа на нежеланите посетители. Описаният по-горе модел се доближава до идеята за сигурност. Тя може да бъде разглеждана като серия от мерки (контроли), фокусирани върху превенцията срещу злосторници и техните нежелани действия спрямо защитаваните активи. В повечето случаи мерките или контролите представляват достатъчно средство за превенция на атаките срещу сигурността на защитаваните активи. В същото време като аксиома се приема, че стопроцентова превенция е невъзможна и доказателство за това са успехите на „злосторниците“ да преодолеят прилаганите контроли или мерки за сигурност. Този факт поражда потребността от изграждане и поддържане на устойчивост или с други думи на способности за отговор на атакуващите, когато те вече са „вътре“ в защитаваните обекти. Важността на устойчивостта става реална когато срещу атаките на опонентите се мисли и действа с разбирането „*не ако, а когато*“.

Определенията, които са приложими и по отношение на системата за сигурност, описват устойчивата система като такава, която притежава способности за отговор и възстановяване след инцидент, запазваща възможността да функционира и извличаща поуки от случилото се, което й дава възможност да се самоусъвършенства и я прави по-силна при бъдещи инциденти. В тази посока на мисли, с концепцията за устойчивост са свързани разбиранията за управление на непрекъснатостта за функциониране на системите.

Ако сигурността и устойчивостта се разглеждат като две отделни неща, то връзката между тях би изглеждала линейна, т.е. първо се появява нуждата от сигурност, а след това нуждата от устойчивост. Възможно е и разбиране, според което устойчивостта включва сигурността. По въпроса за взаимоотношението между сигурност и устойчивост съществуват различни мнения. Едни автори разглеждат първо особеностите на сигурността и като продължение анализират особеностите на устойчивостта. Световният икономически форум в своя публикация разглежда устойчивостта с помощта на бинарен подход, т.е. една система може да бъде едновременно както сигурна, така и несигурна. Според NIST устойчивостта представлява процес, включващ пет фази: идентифициране, защита, разкриване, отговор и възстановяване след инцидент със сигурността. При идентифицирането се говори за развитие на способностите за управление на риска за сигурността. В този смисъл сигурността се разглежда като част от устойчивостта.

В крайна сметка, ако се претеглят различните мнения може да се стигне до обобщението, че устойчивостта е по-общото, по-обширното понятие, което по един или друг начин включва концепцията за сигурност.

БАЛАНСИРАНЕ НА УСТОЙЧИВОСТТА НА СИСТЕМАТА ЗА СИГУРНОСТ

Изграждането на устойчива система за сигурност е свързано с постигане на баланс. Балансирането на устойчивостта намира израз в балансиране на превантивните, детективските и коригиращите контроли или мерки. За да бъде устойчива, системата за сигурност следва да прилага по един балансиран начин горните три вида контроли:

- *превантивни,* за предотвратяване на инциденти със сигурността на активите;
- *детективски*, за своевременно откриване на възникването на инцидент със сигурността на активите;
- *коригиращи*, за отговор и възстановяване на последствията от инцидент със сигурността на активите.

При търсене на баланс между трите вида контроли следва да се отчитат разходите и ползите от мерките за превенция, както и краткосрочното влияние върху устойчивостта на инцидента по време на неговото разкриване и отстраняване. За да се определи какви точно контроли трябва да бъдат приложени следва да се преценят някои конкуриращи се нужди за продължаване на процесите, контролиране на разходите, удовлетвореност на потребителите на продукта „сигурност“, снижаване на риска за устойчивостта. Тези решения следват единна и базирана на оценката на риска стратегия, отговаряща на апетита и толеранса към риска.

При възникване на инцидент със сигурността на активи от системата за сигурност, контролите за превенция губят своята ефективност. В тези случаи нараства значението на детективските и коригиращите контроли, които са част от реакцията/отговора при възникване на инцидент. Двата вида контроли допринасят за намаляване на нежеланите последствия от инцидента.

Устойчивостта на системата за сигурност разчита на добрия баланс между хора, процеси и технологии. Често допускана грешка е прекаленото разчитане на един от тези компоненти, а именно на технологиите и пренебрегване на огромния принос, който могат да имат към устойчивостта добре обучените и тренираните професионалисти и правилно

проектираните процеси. Наличието на пропуски, слабости, уязвимости в един от трите компонента може да компрометира устойчивостта на системата за сигурност като цяло, както и да снижи ефективността на останалите два. Устойчивостта разчита и се базира на подходящ баланс между хора, технологии и процеси, като трите компонента следва да се разглеждат в тяхното единство, с допълваща сила и без пропуски. Като пример, с областта на киберсигурността взаимната връзка между хора, технологии и процеси се описва с помощта на т.нар. „златен триъгълник“.

Връзката между отделните компоненти – хора, процеси и технологии и устойчивостта може да бъде описана по следния начин:

- хора и устойчивост: природата на немалка част от заплахите за устойчивостта на системата за сигурност включва човешкия фактор в различен аспект. Като пример, недобре или неправилно информираните и обучени професионалисти не само, че не са в състояние да противодействат на заплахите, но самите те в определени случаи се превръщат в заплаха за устойчивостта на системата за сигурност.
- *процеси и устойчивост*: процесите, протичащи в системата за сигурност се подчиняват на строги правила и следват стриктни изисквания при тяхното изпълнение. При намиране на мястото на изискванията за устойчивост в хода на създаване на процесите следва да се отчита изповядваната философия, организационната култура, апетита и толеранса към риска и т.н. На практика, при проектиране на процесите трябва да се търси баланс между нивото на риска за сигурността и нивото на ефективност и удобство на извършваните операции в рамките на процесите.
- *технологии и устойчивост*: технологиите автоматизират изпълнението на процесите и облекчават труда на персонала. Не рядко те компенсират слабости в качествата на персонала и пропуски в процесите, с което допринасят за постигане на устойчивост. В същото време, ниското технологично ниво и остарелите технологии създават уязвимости за системата за сигурност, с което намаляват нейната устойчивост.

КОНЦЕПТУАЛЕН МОДЕЛ ЗА УСТОЙЧИВОСТ В СИГУРНОСТТА

Мисиите на системата за сигурност стоят в основата не само на допринасяните ползи, но също така и в основата на концепцията за нейната устойчивост. Мисиите на системата за сигурност се дефинират с помощта на съвкупност от програми, проекти и дейности, които се изпълняват с цел създаването на продукта „сигурност“, който е предназначен за потребителите в лицето на гражданите, фирмите и т.н. Мисиите могат да бъдат определени също така като част от ресурсите на системата за сигурност, които допринасят за изпълнение на поставените общи цели. От друга страна, всяка мисия има собствена цел, с изпълнението на която подпомага постигането на стратегическите цели на системата за сигурност. Провалът при изпълнението на целите на отделните мисии застрашава постигането на мисията на системата за сигурност като цяло.

За да бъде продуктивен, всеки процес в системата за сигурност се нуждае от активи, които се явяват суровини за процеса. Никой процес не може да постигне своите резултати без:

- персонал, който изпълнява или контролира дейностите от съдържанието на процесите;
- данни и информация, които захранват процесите или които се получават като резултат от процесите;
- технологии, които поддържат и автоматизират изпълнението на процесите;

- инфраструктура, с помощта на която процесът генерира продукт, който се предоставя на потребителите.

За да се определят изискванията за устойчивост към процесите, протичащи в системата за сигурност, трябва да се определят активите от гледна точка на тези процеси и след това да определят изискванията към тяхната устойчивост.

Човешкият фактор (професионалистите) на системата за сигурност е жизнено важен за функционирането на всеки процес. Персоналът участва в изпълнение на процесите и контролира постиганите резултати, като при необходимост въвежда нужните корекции. Като ресурс за процеса, персоналът може да бъде класифициран по различни начини, като пример вътрешен и външен спрямо конкретния процес.

Данните и информацията, независимо на какъв носител са, правят възможно протичане на процеса. В същото време те могат да бъдат и продукт на този процес. Могат да се различават по формат, по обем и по степен на конфиденциалност.

Ролята на технологиите е да поддържат процесите, като в този аспект могат да имат директен или индиректен принос.

Инфраструктурата включва физическите активи, които са в помощ на протичането на процесите. Често пъти една и съща инфраструктура поддържа повече от един процес.

Подходящото описание на активите подпомага дефинирането на изискванията за устойчивост и в същото време осигурява изпълнението на тези изисквания. Описанието на активите прави възможно определянето на техните граници, на взаимодействието между тях, на отговорностите за тяхната устойчивост.

Всеки ключов актив на системата за сигурност следва да бъде описан с максимално възможна подробност. В общия случай описанието на активите за един процес включва:

- видове необходими активи (хора, информация, технологии, инфраструктура);
- нива на чувствителност за активите, особено за информацията;
- местоположение на активите и кой отговаря за тях;
- форма или формат на активите;
- място, където се съхраняват резервните активи, като пример, резервните копия на информацията;
- процеси, които ползват активите;
- стойност на активите в количествени и качествени измерители.

Към горните показатели за описание на активите могат да се добавят изискванията за тяхната устойчивост.

За да се определят изискванията за устойчивост на процесите, протичащи в системата за сигурност, следва много добре да се разбира тяхната връзка с активите. Свързването на процесите с активите помага да бъде открито наличието на т.нар. критични точки и зависимости. Тези зависимости са породени от факта, че е възможно различни процеси да споделят едни и същи активи. Зависимостите следва да бъдат разрешавани с помощта на мерки за устойчивост и стратегии за тяхното прилагане.

При промяна в активите, осигуряващи даден процес, могат да се наложат промени в изискванията за устойчивост. За оценяването на тези промени са нужни критерии, които покриват и четирите групи активи. Като примери за значими промени в активите, които биха повлияли върху устойчивостта на протичащите процеси могат да бъдат:

- промени в структурата или персонала в системата за сигурност с ангажименти към устойчивостта на процесите;
- значими промени в използваните технологии;

- наличие на нова информация, свързана с процеса;
- придобиване на нови активи и т.н.

МЕНИДЖМЪНТ НА АКТИВИТЕ КАТО ЧАСТ ОТ МОДЕЛА ЗА УСТОЙЧИВА СИСТЕМА ЗА СИГУРНОСТ

За да могат да подпомагат процесите в системата за сигурност съответните активи трябва да бъдат налични и достъпни. Терминът достъпност засяга системите, персонала, потребителите, администраторите, които поддържат или използват съответния процес. В общия случай, мениджмънтът на активите изисква балансиране на потребностите на системата за сигурност с подходяща съвкупност от контроли за устойчивост на процесите. При високо ниво на защита се намалява достъпът до процесите и тяхната продуктивност. Обратното също е вярно. При ниско ниво на защита се увеличава рискът от неоторизиран достъп до процесите, което отново занижава тяхната продуктивност. Основният инструмент, с помощта на който се постига баланс в управлението на процесите и свързаните с тях активи е управлението на достъпа. Привилегиите и ограниченията за достъп са механизмите за осигуряване на продуктивност на процесите и за тяхната устойчивост. Привилегиите и ограниченията за достъп се реализират с помощта на административни, логически и физически контроли.

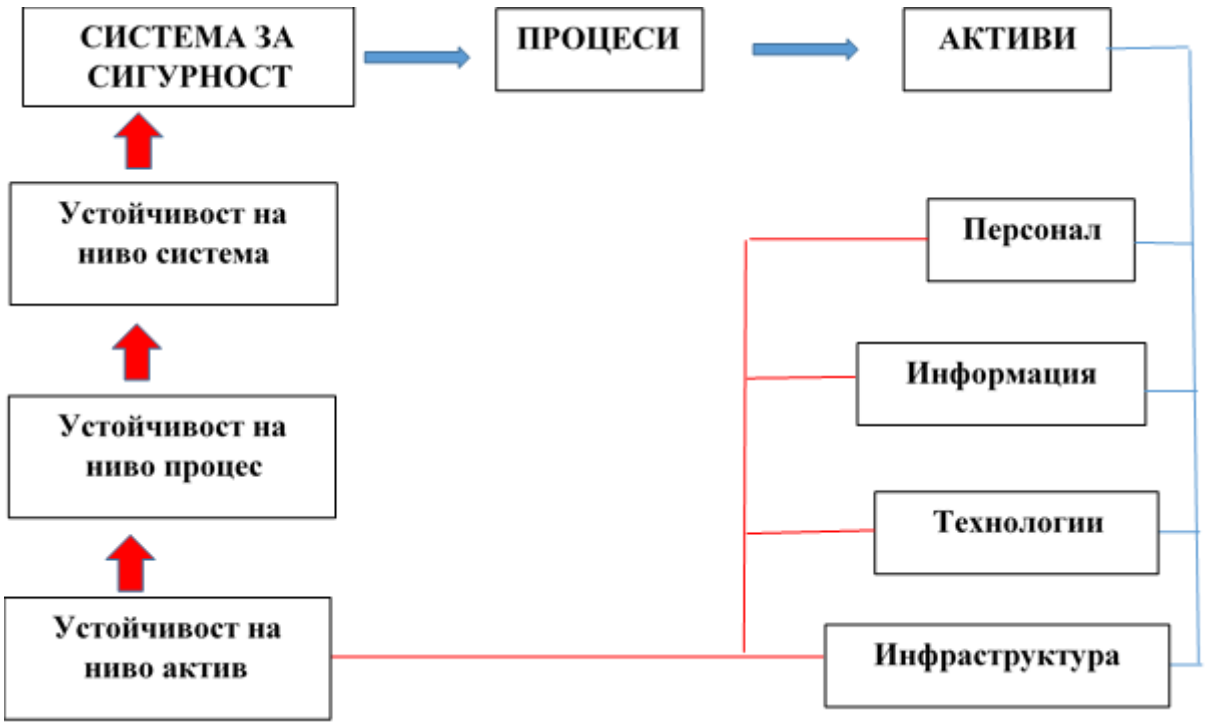
Контролите за достъп се различават от привилегиите и ограниченията на достъпа. Те се проектират и внедряват с отчитане на изискванията за устойчивост на процесите, т.е. те са механизмите, които въвеждат в сила изискванията за устойчивост по отношение на конфиденциалността, интегритета и наличността. За да се поддържат контролите за достъп актуални спрямо променящата се среда се осъществява т.нар. мениджмънт на достъпа. Привилегиите и ограниченията на достъпа определят нивото за достъп до активите в съответствие с изискванията на позицията на персонала и изискванията за устойчивост на процесите и активите. Те трябва добре да бъдат управлявани за да се снижат уязвимостите, предизвикани от неоторизираното използване на активите.

Устойчивостта на активите и на поддържаните от тях процеси от съдържанието на системата за сигурност зависи от ефективността на проектираните, внедрени и управлявани вътрешни и външни комуникации. Комуникациите се явяват част от управлението на устойчивостта чрез участието им в процесите за управление на риска, мениджмънт при инциденти, непрекъснатост на бизнеса, осигуряване на съответствие и т.н.

РАЗРАБОТВАНЕ НА ИЗИСКВАНИЯ ЗА УСТОЙЧИВОСТ НА СИСТЕМАТА ЗА СИГУРНОСТ

Целта пред разработването на изисквания за устойчивост на системата за сигурност е идентифициране, документиране и анализиране на изисквания за устойчивост на протичащите процеси и на поддържащите ги активи. Изискванията за устойчивост представляват характеристики, състояния, способности, които следва да са налични и да се развиват по отношение на активите, така че тези активи да остават адекватни на потребностите на процесите и на мисиите на системата за сигурност. На практика, изискванията за устойчивост са насочени към четирите групи активи – хора, информация, технологии, инфраструктура. Те представляват основата или базата за защита на активите от заплахи и поддържане на активите в състояние, отговарящо на изискванията на процесите.

Стратегическият мениджмънт на устойчивостта на системата за сигурност започва с формулиране на изискванията за устойчивост на ниво система като цяло, на ниво отделни процеси и на ниво отделни активи (виж фиг. 1). Изискванията за устойчивост отразяват стратегическите цели пред системата за сигурност, нивото на апетит към риска, критичните фактори за успех, оперативните ограничения.



Фиг. 1. Структуриране на изискванията за устойчивост на системата за сигурност.

Изискванията за устойчивост на системата за сигурност като цяло следва да бъдат съобразени и да отговарят на потребностите от сигурност на заинтересованите групи лица и на съществуващите ограничения. Те покриват всички аспекти на системата за сигурност. Източници за тази група изисквания за устойчивост могат да бъдат закони, политики, планове, програми и регулации. Изискванията за устойчивост на отделните процеси, протичащи в системата за сигурност, се създават при отчитане на предназначението на процеса и връзките му със системата за сигурност и с поддържащите активи. Фокусът е върху наличността/достъпа до процеса и възможностите за неговото възстановяване в случай на инцидент. Изискванията за устойчивост на активите защитават активите с цел да се осигури достъп и работоспособност на процесите. Понякога към различните активи могат да съществуват изисквания за устойчивост, които влизат в конфликт, особено когато едни и същи активи поддържат повече от един процес.

Съществуват различни начини за определяне на изискванията за устойчивост. Стратегическото планиране може да даде изискванията за устойчивост на системата за сигурност като цяло. Изискванията за устойчивост на отделните процеси могат да бъдат зададени от оперативните мениджъри. Изискванията за устойчивост на активите могат да бъдат определени на базата на резултатите от анализа и оценката на риска. Съвкупността от определените изисквания за устойчивост на системата за сигурност следва да бъде анализирана в посока разкриване на съществуващи конфликти и взаимни зависимости, които трябва да бъдат оценени по отношение на влиянието и приноса към постигане на мисията на системата за сигурност.

МЕНИДЖМЪНТ НА ИЗИСКВАНИЯТА ЗА УСТОЙЧИВОСТ НА СИСТЕМАТА ЗА СИГУРНОСТ

Целта е да се осигури достатъчно ефективен мениджмънт на изискванията към ключови процеси на системата за сигурност и на свързаните с тях активи, както и да се определят несъответствията между тези изисквания и дейностите, които се изпълняват за да отговори на тях. Мениджмънтът на изискванията за устойчивост на системата за сигурност обхваща техния пълен жизнен цикъл: от определяне на потребностите, през разработване, прилагане, наблюдение и измерване на резултатите, до извършване на необходимите промени в изискванията за устойчивост.

Мениджмънтът на изискванията за устойчивост на системата за сигурност включва:

- постигане на увереност в това, че разработените изисквания за устойчивост на трите нива (система, процеси, активи) остават достатъчно ефективни при промени в средата;
- извършване на промени в установените изисквания за устойчивост при възникване на необходимост;
- усъвършенстване на изискванията за устойчивост при настъпили промени в целите пред системата за сигурност спрямо процеса за разработване на изисквания за устойчивост.

Изискванията за устойчивост на системата за сигурност се управляват спрямо активите посредством:

- идентифициране на необходимите промени в съществуващите изисквания за устойчивост;
- постигане на общо споделено разбиране за изискванията за устойчивост между всички заинтересовани лица;
- поддържане на съответствието между изискванията за устойчивост и съответните активи и процеси;
- предприемане на коригиращи действия когато практиката не изпълнява изискванията за устойчивост.

ЗАКЛЮЧЕНИЕ

Като едно от най-надеждните доказателства, практиката показва, че постигането на сигурност не изчерпва очакванията за създаване и поддържане на среда, осигуряваща продуктивност и просперитет. Инцидентите и кризите със сигурността в различни нейни аспекти поставят изискване за изграждане на устойчива система за сигурност със способности за адаптиране към и възстановяване след настъпили нежелани събития. Изграждането на устойчива система за сигурност изисква създаването на модел, върху който да се проведат дискусии и да се структурират политики, стратегии, програми, планове и реални мерки.