IT4Sec Reports 109
http://dx.doi.org/10.11610/it4sec.0109

Защо всяка организация се нуждае от политика и програма за информационна сигурност

Михаел Димитров

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

София, декември 2013 г.

Михаел Димитров, Защо всяка организация се нуждае от политика и програма за информационна сигурност, *IT4Sec Reports* 109 (София, Институт по информационни и комуникационни технологии, декември 2013 г.), http://dx.doi.org/10.11610/it4sec.0109.

IT4SecReports 109 „Защо всяка организация се нуждае от политика и програма за информационна сигурност“. Текстът се фокусира върху причините, налагащи на организациите да притежават политика и програма по информационна сигурност с оглед постигането на конкурентно преимущество, базирано на подобрени възможности за адаптация. Първо се разглежда понятието информационна сигурност, за да се представи каква е целта преследвана от страна на организациите. След това се описва същността на организациите като участници съществуващи в конкурентен контекст на средата. По този начин се формулират конкретните начини по които информацията придобива значимост от представяната гледна точка. Дадени са примери, които демонстрират необходимостта от изготвяне на политика и програма по информационна сигурност, описващи уязвимости и заплахи, по отношение на които липсата на адекватни мерки за противодействие би могла да доведе до неспособност на организациите да постигат своите цели.

IT4Sec Reports 109 “Why the Organization Needs Information Security Policy and Programme“. This report outlines the reasons why each organization needs to adopt an information security policy and an information security programme, emphasising the competitive advantages based on improved adaptation capabilities. First, it examines the concept of information security. On that basis, the author represents possible formulation of organizational objectives. The examination of organizational activities in a competitive context allows to formulate specific ways in which information becomes of utmost significance. The report includes examples demonstrating the need to establish an information security policy and an information security programme, including description of threats and vulnerabilities that, unless adequately managed, could decrease the organizational capabilities to achieve their goals.

Keywords: information security, organization, adaptability, information, information security policy, information security programme, threat, vulnerability, resources.

Михаел Димитров е студент в магистърската програма по „Национална и международна сигурност” на Нов Български Университет.

ISSN 1314-5614

Управлението на организациите включва редица аспекти и проблеми, сред които нараства значимостта на въпросите засягащи важността на информационната сигурност, както и невъзможността организациите успешно да постигат своите цели при отсъствието на политика и програма, които да гарантират изграждането и поддържането на желаното състояние на защитеност на информацията[1]. В центъра на изследването се поставят организациите, независимо от техния характер, от гледна точка на политиките и програмите по информационна сигурност, които следва да им предоставят устойчиво функциониране и конкурентни преимства. В хода на изследването се дефинират и подлагат на анализ причините, които налагат организациите да притежават както политика, така и програма по информационна сигурност. Постигането на целта на изследването преминава през разглеждане на същността и съдържанието на понятието информационна сигурност, същността на организацията, описание на взаимовръзката между политика и програма по информационна сигурност, както и разкриване на конкретните модуси на значимост на информацията от възприетата гледна точка.

С оглед постигането на желаното равнище на представяне по отношение на изследвания обект е необходимо да се обърне внимание първо на това, какво всъщност представлява информационната сигурност в така установения контекст. Отчитайки релационната природа на това понятие, явно то ще бъде неотменно обвързано с организацията, явяваща се негова отправна точка, като в зависимост от характера на нейните цели и обхватност, то би придобивало в известна степен различни значения във възможните конкретни варианти, но все пак запазвайки своето основно съдържание. Така информационната сигурност може да бъде дефинирана като защита на информацията и поддържащата я инфраструктура от случайни или планирани въздействия (реализирани по естествен начин или предизвикани от дейността на човека), които могат да доведат до вреди с неприемлив мащаб[2]. При увеличаване на равнището на приближение на изследването се използват и основните категории с които борави информационната сигурност – достъпност, неприкосновеност, конфиденциалност и автентичност[3]. По този начин се получава възможността за постигане на по-голяма точност при представянето на изследвания обект чрез въвеждането на релевантни примери, изразяващи конкретни заплахи и уязвимости.

Насочвайки усилията си към разкриване на понятието организация, неизбежно следва да се засегне и присъщата страна на човешкото присъствие да организира себе си във фрагментирани общности въз основа на различни критерии, сред които основните са свързани с характера на използваните системи от знаци за комуникация, изграждащивпоследствие допълнителни конотативни натрупвания, увеличаващи равнището на разграничение и враждебност, създавайки конкурентен контекст на средата. Освен това, тези разделения макар и създаващи обособени цялости, в крайна сметка водят до състояние, при което изграждащите ги елементи също се стремят към заемане на превъзхождащи позиции вътре в тях, което прави конкурентността пронизваща организациите, представяйки ги като изграждани от такива притежаващи по-ограничен характер. Тези мисли позволяват организацията да се разглежда като винаги колективно присъствие, можещо да бъде както не-държавно, държавно, така и наддържавно, но при всички положения съществуващо в конкурентна среда, поне доколкото не се възприема глобален обхват на погледа, въпреки че дори и тогава конкурентната среда ще е налице, но ще се превърне във вътрешна. Този образ на организациите като изразител на човешкия стремеж към подобряване на притежаваните възможности, донякъде подвластни на Дарвиновите принципи, произвеждащи нова организационна генетика, чиито мутации

---

1 Настоящият материал представя резултатите от проведено изследване в областта на информационната сигурност на организациите

2 Георгиев, В., Анализ на сигурността в информационното пространство, София, 2013 г., 24

3 Пак там, с. 24-25

постоянно биват тествани от конкурентните пространства, предоставя възможността да обвържем организациите чрез еволюцията със способностите за адаптация[4].

Разглеждайки организацията като изградена от система за взимане на решения, оперативна система и информационна система, особено отчитайки дефиницията на последната като съвкупност от взаимно свързани и взаимодействащи си компоненти, осъществяващи връзката между предходните две системи на организацията и външната система (среда)[5], става ясна значимостта на информацията за постигането на навременна и успешна адаптация спрямо измененията в средата на сигурност. Една толкова важна функция за самото съществуване на организацията не може да бъде оставена без контрол и именно поради това изисква наличието на определени механизми, които да регулират тази дейност като в зависимост от тяхната ефективност толкова по-успешно или неуспешно би било и присъствието. Така ако политиката за информационна сигурност бъде възприета като мисловна конструкция, в която се дефинират целите и съответните стратегии за нейното постигане[6], то наличието й ще се явява фактор, от който в най-голяма степен зависи способността за придобиване и запазване на адаптивност от страна на организацията. Разбира се, политиката от своя страна изразяваща стратегическата цел да се гарантира информационна сигурност, се нуждае от програма, която да спомага за нейното приложение на оперативно и тактическо равнище, като разпределя конкретните подцели насочени към ограничаване на уязвимостите и елиминиране на заплахите и моделиране на поведението на останалите участници в конкурентното пространство. Основното противоречие в това отношение се изразява чрез необходимостта внимателно да бъдат определяни ресурсите необходими за осъществяването на определени намеси, целящи постигане на информационна сигурност, след което те да бъдат съотнасяни спрямо значимостта им за цялостното функциониране на организацията, с оглед постигане на резултат близък до оптималния при разпределянето на винаги ограничените ресурси.

За да се разгледа в необходимата степен значимостта на политиката и програмата по информационна сигурност за организацията, е необходимо да се пристъпи към увеличаване на приближението на представяне и да се разкрият конкретните модуси на използване на информацията за гарантиране на собствената сигурност, поставяйки ударение именно върху възможностите за адаптация. Така основни характеристики на информацията в това отношения са нейните пълнота, правилност, разпространение, точност и съгласуваност, както и ситуационно обусловените релевантност, навременност и увереност в източниците[7]. Следователно организациите които се стремят към постигане на по-висока адаптивност и успеваемост в конкурентното пространство, независимо от какъв характер е то, следва да притежават информационно осигуряване, отговарящо на посочените характеристики. Имайки предвид сложността на този процес е трудно да си представим организация, която без политика и програма по информационна сигурност, би могла да определя точно информацията от която се нуждае и начините по които да гарантира нейното придобиване, съхранение и използване.

Разбира се, отчитайки вече разкритата интензивност на конкуренцията между организациите, особено когато те са от подобен тип, налага политиката по информационна сигурност да включва и конкретни действия за увеличаване на непрозрачността на притежаваната информация, като в същото време е възможно да се изграждат и способности за повишаване на прозрачността на опонентите и средата. В това отношение се засягат най-вече категориите конфиденциалност и неприкосновеност, като възможните уязвимости и заплахи зависят от обхватността и целите на организацията. Така ако се разглежда участник, притежаващ държавен характер, явно поради същността на средата в която той преследва целите си, интензивността на противопоставяне в разглеждания аспект

---

4 Alberts, D., J. Garstka, R. Hayes, D. Signori, UnderstandingInformationAgeWarfare, CCRP, 2001 г., xiii

5 Георгиев, В., Анализ на сигурността в информационното пространство, 15

6 Пак там, с. 29

7 Alberts, D., J. Garstka, R. Hayes, D. Signori, UnderstandingInformationAgeWarfare, 95-97

би достигнала най-високо равнище, доближавайки се до състоянието на информационна война. Тогава уязвимостите ще варират от слабости в санкционирането на достъпа до носителите на информация, до неконтролирането на косвени признаци, можещи отново да предизвикат разкриване на реализирани действия или възприети цели. В такъв случай и конкретните заплахи могат да се изразят чрез дейностите на опонентите по разузнавателно наблюдение, наблюдение на обкръжаващата среда, разузнавателно пътуване, добиване на веществени носители на информация, както и чрез добиване на информация в електронноинформационна среда. Ако насочим вниманието си към организации притежаващи по-ограничен обхват, тогава вероятно интензивността би била ограничена, именно поради наличието на субект, създаващ правила регулиращи възможните взаимодействия, но същността на уязвимостите и заплахите ще се запази, като единствено целите ще бъдат променени (разкриване на търговска тайна, целеви групи на продукти/услуги, авторско и патентно право).

Освен това самото разпространение на информацията вътре в организацията, имайки предвид нейния характер на колективно присъствие, налага съществуването на правила, въз основа на които да се осъществява този процес, за да се ограничи доколкото е възможно вероятността нейни представители да разкриват информация, която би могла да нанесе значителни вреди. Тук отново се засягат основно категориите конфиденциалност и неприкосновеност, като уязвимостите са свързани с нарушаването на принципа за минимизиране на привилегиите, представляващ предоставяне на служителите само на онези права, които са необходими за изпълнение на техните служебни задължения[8]. Заплахите от своя страна могат да се изразят чрез опасността от създаване на разузнавателни позиции вътре в организацията, които да бъдат използвани за добиване на информация или за нерегламентирано изменение на нейното съдържание. Това налага в политиката по информационна сигурност да бъде съобразен достъпа на служителите до чувствителна информация, за да се намали вероятността от “пробив”, а при евентуален такъв да е налице възможност за бързо идентифициране на нарушителите и ограничаване на последствията, както и своевременно прекратяване на вредното въздействие.

От съществено значение е устойчивостта на информационната система на организацията и снижаване на възможностите за разстройване на нейното функциониране. В това отношение отново евентуалната липса на политика и програма по информационна сигурност би допринесла за невъзможност адекватно да се оцени и анализира съществуващия риск и при условия на недостатъчност на ресурсите биха възникнали уязвимости за информационната сигурност. Разглеждането на информационната сигурност от тази гледна точка е свързано с категориите достъпност и неприкосновеност. Уязвимостите следва да бъдат определени като произлизащи от слабости в апаратното и програмно осигуряване на информационните системи, както и от пропуски по отношение на процедурите, имащи за цел защита на критичната информационна инфраструктура в организацията. Заплахите от своя страна могат да представляват физически намеси за разрушаване на компонентите на информационната система или действия, целящи нейното забавяне и объркване чрез използването на вредоносно програмно осигуряване. Постиганият по този начин отказ на достъп до услуги е възможно да бъде използван в качеството си на средство при реализирането на противоборство с висока интензивност между държави или при конкуренцията между бизнес организации с оглед увеличаване на притежавания от тяхна страна пазарен дял.

Дали и в каква степен да бъде споделяна притежаваната информация от организацията е друг въпрос, изискващ да бъде включен в политиката и програмата по информационна сигурност, макар и отчитайки че при него ситуационният контекст би бил от особено значение. В това отношение могат да се разглеждат най-малкото два варианта, като при първия организацията споделя информация с други организации, за да намали вероятността от конфликт, или за да постигне изгодно за нея състояние на

[8] Георгиев, В., Анализ на сигурността в информационното пространство, 69

взаимоотношения в средата на присъствие. Тук трябва да се отбележи, че начинът по който бива възприемано и разбирано поведението на останалите участници в конкурентното пространство до голяма степен предопределя избора на стратегия за взаимодействие с тях. От своя страна изграждането на образи за останалите организации, представлява дейност изцяло зависима от наличната информация. Именно поради тази причина, макар и да изглежда като противоречие на вече представения стремеж за увеличаване непрозрачността на притежаваната информация, при дадени обстоятелства разкриването на точно определени факти може да допринесе за ограничаване на враждебността и успешно постигане на поставените цели. Тук от ключово значение е категорията конфиденциалност, поради необходимостта от прецизно определяне и съотнасяне на положителните и отрицателните страни, произлизащи от разкриването на съответната информация и рискът, изразяващ се чрез вероятния конфликт.

При вторият възможен вариант, въздействия с негативен характер произлизащи от дейността на организацията и застрашаващи външната й среда биха наложили разкриване на информация за конкретните източници на заплаха, интензивност и възможности за ограничаване на последствията, ако разбира се не е налице умисъл. Именно тук е важно да се определи дали външният натиск е по-опасен от разкриването на информация за конкретно събитие или дейност, а това налага притежаването на политика и програма по информационна сигурност, които да осигуряват ако не готов отговор, то поне сценарии, служещи като основа за взимане на решение в подобни ситуации. В този случай отново ударението е поставено върху конфиденциалността и макар причината за това да е друга, необходимостта от прецизност при разкриването на информация се запазва. Пример в това отношение е евентуалното притежаване от страна на организацията на потенциално опасни обекти, реализиращи дейност, която при неспазване на технологичните правила за нейното извършване може да причини щети в големи размери, които надхвърлят обхватността на нейните граници. Това налага разкриването на вече посочената по-горе информация, но все пак отчитайки нейната чувствителност и постоянно съотнасяйки я към външния натиск. Постигането на търсения баланс в това отношение е значително предизвикателство за организациите изправени пред подобни проблеми, но при всички положения омаловажаването на настъпили инциденти или аварии пред останалите участници в средата на присъствие най-вероятно би довело до по-големи вреди и за самата организация, независимо дали тя притежава не-държавен, държавен или наддържавен характер.

Не бива да се пренебрегва значимостта на информацията за изграждането на визия на организацията, тъй като в зависимост от това как останалите участници я възприемат, ще се променят и техните стратегии за взаимодействие, което при оказване на успешно въздействие може да предизвика желани реакции, повишаващи не само информационната сигурност, но и сигурността на съответното колективно присъствие като цяло. В известна степен подобни намеси наподобяват тези, свързани с разкриването на информация с оглед намаляване на вероятността от конфликт, но тук целта може да се определи като по-широка, тъй като усилията са насочени към моделиране на поведението на останалите участници в конкурентното пространство. Предприемането на такива действия, които граничат с операциите по дезинформация и психологическа война, могат да се определят като намиращи се на границата на полето на познавателен интерес, но за да се получи желаното равнище на изчерпателност при представянето, следва да бъдат макар и частично засегнати. От тази гледна точка отново категорията конфиденциалност притежава водеща роля, поради необходимостта не толкова да се избегне разкриване на чувствителна информация, а на такава която е в противоречие с желания образ, който следва да бъде изграден за организацията. Реализирането на подобна функция е присъщо на повечето бизнес организации и на държавните институции, които се стремят да постигат своите цели чрез дипломатически средства, но по един или друг начин тя присъства в дейността на всеки един участник в конкурентното пространство. Все пак разликите в зависимост от това дали е налице осъзнато отношение спрямо важността на този аспект, предопределят до голяма степен неговия успех или съответно неуспех.

От направените изследвания става ясно, че всяка организация независимо от своя характер, пространствен обхват и цели, следва да притежава политика и програма по информационна сигурност, тъй като в противен случай ще изгуби значителна част от възможностите си за въздействие върху средата, увеличавайки неимоверно динамичните си габарити и оставяйки до голяма степен своето бъдеще в ръцете на опонентите си, които използвайки по-успешно информацията, биха постигали конкурентно преимущество, базиращо се на подобрени възможности за адаптация.

ЛИТЕРАТУРА

Георгиев, В., Анализ на сигурността в информационното пространство, София, 2013г.

Alberts, D., J. Garstka, R. Hayes, D. Signori, Understanding Information Age Warfare, CCRP, 2001 г.