Съвременни тенденции при формиране на политики за информационна сигурност

Ивайло Николов

Contemporary trends in the formation of policies for information security: *The dynamic development of information and communication technologies in the last decade set a number of new requirements to the rules and procedures for the formation of information security in organizations. Increasing computer threats on the Internet necessitate timely and adequate update of information security policy to ensure the security of information, regarding its collection, storage, processing and distribution.*

Key words: *Information Security,Model, Information Security Systems.*

ВЪВЕДЕНИЕ

Динамичното развитие на информационните и комуникационни технологии в последното десетилетие постави редица нови изисквания към правилата и процедурите за формиране на информационна сигурност в организациите. Растящия брой компютърни заплахи в Интернет налагат своевременно и адекватно актуализиране на политиките за информационна сигурност с оглед гарантиране сигурността на събираната, съхранявана, обработвана и разпространявана информация.

Настоящият доклад се явява продължение на изследванията [1,2], проведени в областта на информационната сигурност и може да намери приложение при разработка и внедряване на системи за информационната сигурност.

ПОЛИТИКА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Политика за информационна сигурност се нарича съвкупността от документирани решения, приети от ръководството на организацията и насочени към защита на информацията и асоциираните с нея ресурси [4].

Създаването и актуализирането на различни по своя характер политики за информационна сигурност е динамичен процес, които зависи от информационните и комуникационни технологии и свързаните с тяхното развитие рискове за използвания информационен ресурс. Политиките за информационна сигурност отразяват както спецификата в дейността на организациите, така и противодействието на глобалните заплахи, възникващи в процеса на развитие на Интернет и комуникационната свързаност на обществото.

Пример на политика за сигурност е политиката за физически контрол на достъпа или за унищожаване на технически носители на информация, политика за защита на личните данни и т.н.. Правилата и процедурите за изграждане на информационна сигурност са тясно свързани с конкретни стандарти на Международната организация по стандартизация (ISO). Спазването на тези стандарти гарантира, че продуктите и услугите са безопасни, надеждни и с добро качество.

СТАНДАРТИ ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Стандартите от семейството на ISO 27000 са серия стандарти, които помагат на организациите да поддържат информационните си активи защитени.

Стандартът ISO 27001 цели осигуряване и подобряване на системата за управление на информационната сигурност (СУИС). Проектирането и изпълнението на информационна система за управление на сигурността на организацията зависи от нуждите на организацията, целите и изискванията за сигурност на използваните организационни процеси, както и от размера и структурата на организацията.

Стандартът ISO 27002 включва в себе си основни елементи на отменения към

настоящия момент стандарт ISO 17799, наречен практически кодекс за информационна сигурност. По същество той очертава стотици потенциални контролни механизми, които могат да бъдат реализирани, на теория, при спазване на указанията, предоставени в рамките на ISO 27001. Стандартните очертават възприетите норми и принципи за иницииране, прилагане, поддържане и подобряване на управлението на информационната сигурност в рамките на организацията. Действителните контроли, изброени в стандарта са предназначени да отговорят на специфичните изисквания, установени чрез официална оценка на риска. Стандартът е предназначен също да предостави указания за развитието на организационни стандарти за сигурност и ефективни управленски практики за сигурност и да помогне за изграждане на доверие в между-организационни дейности.

Актуалната версия на ISO 27002 съдържа 114 контроли, разработени в областта на информационните технологии, комуникации, здравния сектор, производството и т.н. Основните секции са: структура, политиката на сигурност, организиране на информационна сигурност, управление на активи, контрол на достъпа, криптографията, операции за сигурност, комуникационна сигурност, управление на информационната сигурност при инциденти и други

Целта на ISO 27003 е да осигури както помощ при развитие, така и насоки за въвеждането на система за управление на информационната сигурност. Заглавието на стандарта в момента е: "Информационни технологии – техники за сигурност. Насоки за прилагане на системата за управление на информационна сигурност.

Стандартът ISO 27004 предоставя насоки за разработване и прилагане на мерки за измерване и оценка на ефективността на системата за информационна сигурност. Документът е предназначен да помогне на организацията да установи ефективността на изпълнението на своята система за управление на информационна сигурност, като обхваща сравнителен анализ и насоки за представянето му. Официалното наименование на стандарта е: "Информационни технологии - техники за сигурност - Управление на информационната сигурност - Измерване"

ISO 27005 е стандарт, покриващ изискванията за управление на риска за информационна сигурност в организацията. Стандартът дава насоки за управление на риска на информационната сигурност, по-специално в подкрепа на изискванията на системата за управление на информационната сигурност, определена от ISO 27001.

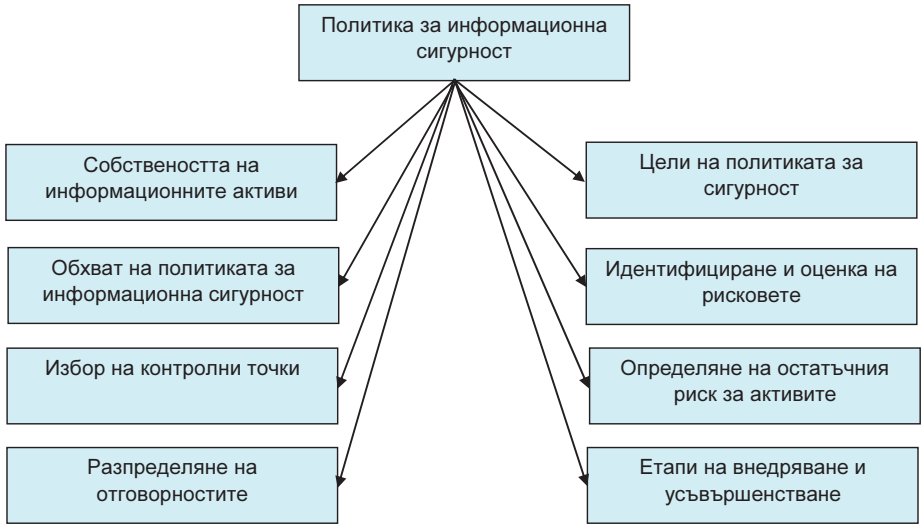
Стандартът ISO 27005 се състои от 55 страници и е приложим за всички видове организации. Той не предоставя и не препоръчва конкретна методология за изграждане на информационна сигурност. Това зависи от редица фактори, като например действителния обхват на системата за управление на информационната сигурност, или от сектора в който се прилага - промишленост, търговия, образование и други.

Стандартът ISO 27006 предлага насоки за акредитацията на организациите, които предлагат сертифициране и регистриране по отношение на системите за управление на информационна сигурност. Официалното му заглавие е "Информационни технологии - Техники за сигурност. Изисквания към органите, извършващи одит и сертификация на системи за управление на информационната сигурност". Документа се състои от 10 глави и четири приложения.

СЪДЪРЖАНИЕ НА ПОЛИТИКАТА ЗА ИНФОРМАЦИОННА СИГУРНОСТ

Съвременните условия на глобални интернет заплахи за информационната сигурност [5,6,7] като например компютърни атаки от типа „отказ на обслужване”, наличие на зловреден софтуер, кражба на данни, включително персонални, номера на кредитни карти, комерсиален софтуер и други, налагат все по-динамично и

целенасочено организациите да поставят като основна цел защита на притежаваните от тях информационни ресурси. На фиг. 1 е представена обобщена схема на съдържанието на политика за информационна сигурност, която може да бъде приложена в организациите при описание спецификите на конкретната дейност по осигуряване на информационна сигурност.



Фиг. 1. *Обобщена схема на политика за информационна сигурност*

При определяне собствеността на информационните активи трябва стриктно да се спазват законодателните норми и правила, с оглед недопускане на противоречие между утвърдените вътрешни правила в организацията и съответния нормативен документ. Организациите, следвайки изискванията на националното и европейско законодателство са силно зависими в прилагането на по-рестриктивни мерки за информационна сигурност. Това налага националните правителства да предприемат сериозни мерки по отношение промяна на нормативната уредба в посока криминализиране на по-широк кръг от компютърни престъпления в съответствие със съвременните методи на компютърни атаки и кибер престъпления. Начините за прилагане на правни политики в организациите се изчерпват в разработката и внедряването на вътрешни правила в различните направления за информационна сигурност.

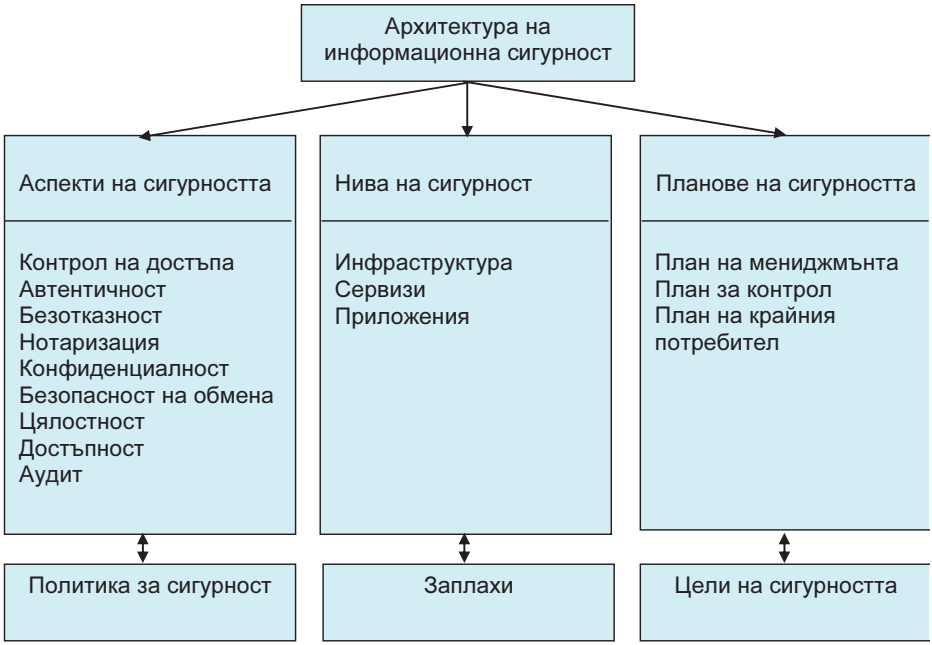
Определяне на обхвата на политиката на информационна сигурност, целите, контролните точки, отговорността, както и рисковете в различните етапи на разработка и внедряване на политиката се причисляват към т.нар. организационно-технически дейности. Те включват редица организационни и технически (хардуерни и софтуерни) методи и средства за осигуряване на информационна сигурност.

Гарантирането на информационната сигурност в организациите е свързано с планиране и реализиране на конкретен финансов ресурс за реализиране на информационна сигурност. Закупуването на съвременна комуникационна техника, антивирусен софтуер, защитни стени и прочее е задължителен елемент при осигуряване на информационна сигурност. Целия набор от методи и средства изисква финансови средства, които всяка организация следва да планира и разходва за защита на използвания информационен ресурс.

МОДЕЛ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Моделът на информационната сигурност се състои от три архитектурни нива [3]: системно, логическо и концептуално.

Модел на архитектурата на информационна сигурност, съгласно препоръки X.800 съдържат следните елементи (Фиг. 2)



Фиг. 2. *Модел на архитектурата на информационна сигурност*

Моделът дава отговор на три съществени за информационната сигурност въпроса [3]:

- Какви видове защита са необходими и против какви заплахи;
- Какви типове оборудване и услуги трябва да бъдат защитени;
- Какви типове дейности трябва да бъдат защитени.

Изследванията [1, 2] доказват, че представения модел отразява в максимална степен изискванията към информационната сигурност.

ЗАКЛЮЧЕНИЕ

Въз основа на изследванията [1,2] и специфичните изисквания, заложени в стандартите от семейството на ISO 27000, бихме могли да направим следните изводи, гарантиращи надеждност при формиране на политики за информационна сигурност:

1. Приложението на модела за информационна сигурност [3], съгласно препоръки X.800 гарантира осигуряване сигурност на информационните ресурси в организациите.

2. Необходимостта от навременни изменения на Наказателния кодекс в областта на компютърните престъпления се оказват наложителни за гарантиране надеждността и нормалното функциониране на организациите. Наличието на

законодателни изисквания, заложени е в Закона за защита на личните данни, Закон за защита на класифицирана информация стандартите, Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи или мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация и т.н.

3. Поради невъзможността от географско разделение на Интернет пространството, належащо се оказва международното сътрудничество в областта на информационната сигурност с цел намаляване на рисковете за организациите, които събират, обработват, съхраняват и разпространяват информация. Активното използване на експертна помощ на страните- партньори за промени в законодателството по отношение на компютърните престъпления и за обмяна на добри практики е важен фактор за гарантиране на сигурност и надеждност на информационните ресурси.

4. Нарастването на компютърните атаки в Интернет поставя всички сектори на обществения живот в риск от нормално функциониране. Общественият интерес за повишаване на информационната сигурност поставят редица изисквания пред научните среди за разработка и внедряване на съвременни методи и средства за информационна сигурност поради наличието на съществен риск за информационните ресурси в организациите от всички сфери на обществения живот.

ЛИТЕРАТУРА

[1] Николов, И. Изследване на компютърни атаки от тип „отказ на обслужване” , Национална конференция с международно участие „Електроника 2015”, София, 2015

[2] Николов, И., Моделиране на системи за инкрементално архивиране при изграждане на информационна сигурност в публичния сектор, Международна научна конференция Техсис 2015, Пловдив, 2015

[3] Туджаров, Х., Архитектура на сигурността, Асеневци, 2010

[4] Туджаров, Х. Информационна сигурност в бизнеса, изд. Асеневци, 2009

[5] http://news7.bg/%D0%9D%D0%BE%D0%B2%D0%B8%D0%BD%D0%B0/%D0%A1%D0%B2%D1%8F%D1%82/%D0%90%D0%BC%D0%B5%D1%80%D0%B8%D0%BA%D0%B0/%D0%91%D0%B0%D0%BD%D0%BA%D0%BE%D0%B2-%D1%81%D0%BB%D1%83%D0%B6%D0%B8%D1%82%D0%B5%D0%BB-%D0%BF%D1%83%D1%81%D0%BD%D0%B0-%D0%B2-%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82-%D0%B4%D0%B0%D0%BD%D0%BD%D0%B8-%D0%BD%D0%B0-%D1%85%D0%B8%D0%BB%D1%8F%D0%B4%D0%B8-%D0%BA%D0%BB%D0%B8%D0%B5%D0%BD%D1%82%D0%B8-_l.n_i.128203_c.29.html#.VdsVuH28pfA, посетен на 20.08.2015 г.

[6] http://technews.bg/article-70917.html#.VdsZo328pfA, посетен на 20.08.2015 г.

[7] http://technews.bg/article-70993.html#.VdsZmH28pfA, посетен на 20.08.2015 г.

За контакти:

инж. Ивайло Николов, докторант в катедра “Комуникационна техника и технологии” на Технически университет - Габрово, тел.:0882 114 289, e-mail: nikolov_i@mail.bg

Докладът е рецензиран.