"Очаквани и реални особености при прилагане на стандарта за управление на сигурността на информацията във фирмите от охранителния бранш"

инж. Бончо Антонов – Алфа Куолити България,
Николета Спасова – Българска Камара за Охрана и Сигурност

Наблюденията ни от тези последни години водят към извод, че у нас има браншове, от които трябва да очакваме да имат силен интерес да въвеждат системи за управление на сигурността на информацията (СУСИ), но данните показват, че този интерес е оскъден, за да не кажем, че на места практически изобщо го няма. Вероятно подвеждащ момент е този, че наименованието на стандарта ISO/IEC 27001 започва с "Информационни технологии ..." и тези организации, чиито бизнес не е в областта на информационните технологии, лесно стигат до решението "това не е за нас". Смисълът трябва да се търси от друга гледна точка – независимо с какъв вид бизнес се занимава една организация, ако ползва в някаква степен "някакви информационни технологии", това би било достатъчно като мотив да се преценява дали информацията, с която се борави е чувствителна и се нуждае от опазване. Един от тези браншове, в които има силен потенциал и широко поле за прилагане на СУСИ, е на фирмите, предлагащи частни услуги за сигурност. В този икономически сектор сигурността на информацията е важна не само за тях, но дори в още по-голяма степен и за техните клиенти.

Ако за други организации сигурността се поддържа като среда за техния основен бизнес, то при фирмите, предлагащи такива услуги, сигурността е не само среда, но и същество на бизнеса.

Охранителните фирми имат "по рождение" здрав и точен рефлекс по отношение на характеристиката "сигурност". Те не само че не афишират, но и добре скриват редица факти и данни за дейността си, които спадат в категорията „чувствителна" информация. При тези фирми нивата на физическа и организационна сигурност са предостатъчно високи, но сигурността при тях трябва да е комплексна (по вид) и балансирана (за различните видове) характеристика, която включва и сигурност на информацията. За резултатността на услуги по охрана може да се съди по допуснати инцидент или по действията в критични ситуации. Логиката подсказва, че един обир може да е успешен само ако се подготви с използване на изтекла ключова информация.

Ако приемем, че в един момент ще бъде осъзната необходимостта и ще възникне достатъчен интерес към системите за управление на сигурността на информацията, трябва да си представим как биха изглеждали системите за сигурност на информацията, усвоявани в охранителния бранш.

Вероятно е добре за целта да се съобразим с някои специфики на бранша. Те са поне три:

1) **регулация** - това е сравнително нов бизнес в икономическото пространство и законовата основа, която легализира частната охранителна дейност, е отскоро, а общата практика в тази област е малко над 20 години. Един от принципите, поставен в Закона за частната охранителна дейност – чл. 3, т. 4, е "осъществяване на *превантивна дейност* въз основа на *анализ на причините и условията* за правонарушения в охраняваните обекти".

На това място трябва да отбележим, че именно превенциите и анализите, които ги предизвикват, са инструменти, залегнали в основата на всички системи за управление по стандартите на ISO – например, ISO 9001 (системите за управление на качеството) и ISO/IEC 27001 (системите за управление на сигурността на информацията).

Въвеждането на системи за управление във фирмите в бранша ще запълни определени празнини в Закона за Частната Охранителна Дейност, в който за качеството на услугите по охрана се разчита на твърде формална основа – лицензи, регистри и контрол от държавни органи.

2) **пазар** - макар и нов, както стана дума по-горе, охранителният бизнес е твърде разпространен и търсенето на такива услуги е задоволително. Данните сочат – издадени са около 1700 лицензи на фирми, а броят на заетите лица – за него няма точни данни – може да е много над 60000 души.

В това виждаме ясни индикации, че браншът е добре развит (като общ обем участници) и че има достатъчен пазар за охранителните услуги. В тази обстановка би трябвало да забелязваме поне две характеристики на пазара – остра конкурентна борба и взискателни към качеството клиенти.

За съжаление, виждаме деформации и в двете характеристики:

- конкурентната борба я виждаме и в полето на качеството и сигурността, но все пак тя основно се изразява чрез налагане на снижаване на цени;
- няма традиционно наложени и развиващи се изисквания към качеството на такива услуги. Клиентелата, и тя е вторачена да гледа къде са най-ниски цените и не пита за качеството.

Последното е особено показателно и учудващо, като се има предвид, че фирмите за сигурност се налага да опазват и информация, принадлежаща на техните клиенти, освен своята собствена.

3) **качество и сигурност** – качеството в дейността на фирмите за охрана се изразява в степента на постигнатата и поддържана сигурност. Сигурността е основна характеристика на качеството на услугите, които предлагат такива фирми. Казано кратко – "сигурност" означава "качество", а "качество" означава "сигурност". Освен това, сигурността, като основна характеристика, трябва да бъде комплексна и балансирана, което означава най-малко следното:

- наред с всички мерки за сигурност, трябва да има и мерки за сигурност на информацията;
- колкото са развити и грижливо поддържани всички мерки за сигурност, толкова трябва да бъдат и мерките за сигурност на информацията.

Търсенето на браншова интерпретация е свързано с постановки на самия стандарт, който казва:

"Внедряването на СУСИ е стратегическо решение за една организация. Създаването и внедряването на СУСИ на организацията зависят от нейните потребности и цели, от изискванията по отношение на сигурността, от включените процеси и от големината и структурата на организацията."

и още

"Също така се очаква внедряването на СУСИ да бъде в съответствие с потребностите на организацията, т.е. елементарен проблем да изисква елементарно решение по отношение на СУСИ."

При това някои от възможните решения за интерпретация се очертават така ...
(ще отделим внимание само на отделни ключови изисквания на стандарта)

Обхват и граници на СУСИ

Стандартът изисква обхватът на СУСИ да бъде изразен чрез четири елемента:

- характеристики на дейността;
- местоположение;
- активи;
- технологии.

Очевидно е, че за "характеристики на дейността" трябва да бъде записано едно към едно онова, което фигурира в издадения лиценз. Същото се отнася и до "местоположение", но тук може да се отчетат някои особености – освен централният офис (или седалище) и поделенията на фирмата, местоположението може да бъде разширено и с площадките на клиентите, където се изпълняват услугите по охрана, особено ако там се ползват технически системи за сигурност. Във връзка с такива технически системи възниква още една особеност – би могло да се приеме, че на такива технически системи, инсталирани при клиента, "собственик" е фирмата за охрана, независимо, че са платени от и са на територията на клиента.

Един от най-сериозните информационни активи на фирма за охрана, който е нужно да се прави специална защита, са изискваните от ЗЧОД "планове за охрана".

Политика по сигурността на информацията

Най-важно е духът и текстовете на тази политика да бъдат съобразени с:

- ЗЧОД и свързаните с него закони и подзаконови актове;
- с фирмената политика по обща сигурност (да се надяваме, че ще има такава !).

По-конкретно, в текстовете на политиката по сигурността на информацията трябва да личи, че са отразени принципите, наложени от ЗЧОД, чл. 3, а именно:
1. зачитане на правата, свободите и достойнството на гражданите;
2. взаимодействие с органите на МВР;3. гарантиране на сигурност и безопасност в охраняваните обекти;
4. осъществяване на превантивна дейност, анализ на причините и условията за правонарушения в охраняваните обекти.
Следващо по важност условие е в Политиката по сигурността на информацията да се включат текстове, които да определят броя и вида на критериите, които ще се използват в работата по оценяване на рисковете. На следващо място Политиката трябва да съдържа текстове, които да насочват към определяне на цели по сигурността.

Цели по сигурността

Те също трябва да кореспондират или да имат и по-преки връзки с *общи цели по сигурността*. При обсъждането и формулирането на целите е най-подходящо да се заложи постановката, че "сигурността" е "качество" и обратно.

Неминуемо трябва да има цели, които се отнасят до удовлетвореността на клиентите. Не е достатъчо да се счита, че щом като на фирмата не е отнет лиценза, то тя работи по най-добрия за клиентите начин. Причината е проста – ЗЧОД изобщо не се занимава с материята "качество" на дейността, а визира единствено няколко груби отклонения като повод за отнемане на лиценз.

И тъй като законите трябва да се уважават такива каквито са, на фирмите остава сами да се погрижат за удовлетворението на клиентите си, като си залагат съответни цели по сигурността и въведат управление на процесите по охрана (с акцент върху процесите по планиране и организация на охраната), включващо показатели за измерване на резултатността.

Оценяване на рисковете

То включва два процеса – Анализ на рисковете и Остойностяване на рисковете с използване на определени и въведени критерии за допустимост – и те трябва да се провеждат по определена и документирана методика. Оценяването приключва с доклад, който документира резултатите.

Подходящо е за методическа основа на оценяването да се ползва стандарта ISO/IEC 27005:2011.

Методиката – нека е собствена, а не преписана отнякъде – е добре да включва поне три момента:

- анализът на рисковете (т.е. систематичното използване на информация с цел да се определят източници на заплахи и да се преценят свързаните с тях рискове) трябва да става в непрекъснат режим или с възможно най-кратка периодичност и, както стана дума по-горе, да включва по обхват и площадките на клиентите;
- освен периодичните "преоценки на рисковете" (те също трябва да са с възможно най-кратък период), да се предвидят и "извънредни преоценки" по повод на конкретни казуси (по реално настъпили събития или инциденти по сигурността на информацията);
- като цяло методиката да е синхронизирана (или да е част от) с методика за оценяване на общите рискове за дейностите по охрана.

Заплахи

Подходящо е да се състави първоначален "генеричен списък" със заплахи, който да послужи като основа при оценяване на рисковете и който би трябвало да подлежи на чести актуализации.

Много е вероятно акцентът при класифициране на заплахите да се падне върху три групи:

- **заплахи, свързани с персонала –**
  - непълно проучване на кандидати за работа,
  - персонал с неформални връзки и отношения,
  - ниско квалификационно равнище (от гл. т. ICT),
  - подценена уязвимост на ICT ресурсите,
  - понижена организационна дисциплина;
- **заплахи, свързани с организацията на дейностите –**
  - връзки и работа с външни страни,
  - недопустимо използване на активи,
  - неразпределени (концентрирани) отговорности,
  - няма или бедна документална основа;
- **заплахи,свързани с ICT практиките –**
  - нередовно или липсващо резервиране на информация,
  - нерегламентирано ползване на преносими носители,
  - небрежно извеждане от употреба на ползвани ICT ресурси,
  - ползване на неразрешени софтуер или достъп,
  - уязвимост от зловредни и от мобилни кодове,

- неодобрено приемане и въвеждане на ICT ресурси (техника, софтуер),
- липса на правила или неправилно съставяне и ползване на пароли,
- неуредена поддръжка на ICT и на поддържащата ги инфраструктура,
- неосигурена наличност (дублиране, резерв) на критичен ICT ресурс.

Документи на СУСИ

Повечето охранителни фирми са малки по числен състав и скромни по общо квалификационно равнище. Това налага да се търси трудно равнодействащо решение между императива да бъдат удовлетворени изискванията на стандарта и получаване на един стегнат и компактен комплект от документи и записи, с които дори и ограничени по числен състав фирми да се справят добре.

Този въпрос е важен, в някаква степен е по-сложен и изисква отделно и задълбочено внимание.

Указанието, което ни дава стандартът в следващата забележка, е ясно разбираемо, но е сложно да се изпълнява по най-подходящия за всяка отделна фирма начин.

ЗАБЕЛЕЖКА 2: В различните организации документацията на СУСИ може да варира в зависимост от:
- големината на организацията и вида на дейността ѝ; и
- обхвата и сложността на изискванията за сигурност и управляваната система

Тук ще се ограничим да посочим само някои от най-общите похвати:

- предпочитаме документацията да е предимно на електронен носител и в електронен формат;
- стремим се да групираме записи, които участват в един и същ процес в тялото на един файл (например, всички записи по оценяване на рисковете плюс доклада от оценяване да са в един файл на MS Excel, но в различни негови листове);
- ревизираме понятието процедура до възможно най-съкратени вид и обем на съдържание;
- прилагаме подход за писане на съставни, т.нар. "master"-процедури, в тялото на които са заложени няколко на брой отделни "mini"-процедури;
- търсим възможно най-кратките форми на изразяване, при които няма загуба на заложения смисъл (дългите документи и сложно изразени изисквания трудно се възприемат и прилагат);
- декларацията за приложимост на механизмите за контрол правим по модела на Приложение А на ISO/IEC 27001.

С особено внимание трябва да се приложат изискванията към документацията:

- да има схема за вътрешна класификация и ползване съгласно схемата;
- да се осигури подходяща защита на документите и записите.

Вътрешни одити

Ако другаде може и да е така, то при охранителните фирми не може да си позволим системата за сигурност да бъде проверявана от формално и неефикасно проведени вътрешни одити. Тук е важно да бъдат осигурени в максимална степен независимост на одиторите и компетентността им.

Би било добре вътрешни одити да се изпълняват от избрани доверени и правоспособни външни експерти, още повече, че одитиранет5о на СУСИ предполага добро познаване и ползване на три стандарта – ISO 19011, ISO/IEC 27007 и ISO/IEC 27008. Не е реалистично да очакваме, че особено в малки по числен състав фирми, ще се намери и подходящ човек с такава квалификация.

В заключение

Връщайки се към заглавието на този материал, трябва да признаем – всъщност повече, ако не всички, са очакваните особености при прилагане на стандарта за сигурност на информацията.

За реалните особености ще имаме право и опит да говорим повече след като целият бранш, а не само отделни – големи и водещи фирми, осъзнае, че не може да предлага на клиентите си продукт "сигурност", ако самият той не работи в условия на комплексна и балансирана сигурност.

Това е естественият път за развитие на охранителните фирми и браншът вече се е насочил по него, за което говори и немалкият брой кандидатствали по програма "Конкурентоспособност" охранителни фирми.

Към тях са нашите пожелания за успехи и напредък, а на останалите – нека пожелаем да имат решителност, да настигат скоро първите и също да успяват

2012.05.02