Интервю на Николета Спасова
за списание "Оръжие, Охрана, Сигурност"
(бр. 9/2010 г.)

инж. Бончо Антонов Поптодоров,
старши консултант по системи за управление

Стандартизираните системи за управление навлязоха в бизнеса и се утвърдиха като важен критерий за доверие във възможностите на фирмите, чрез механизмите за сертификация. Една от тях - Системата за управление на сигурността на информацията (СУСИ) съгласно изискванията на международния стандарт ISO/IEC 27001 започва да добива и у нас важно значение за много фирми и други организации, които работят с информация.

Сега ще поговорим с г-н Поптодоров по темата за сигурността и дали това е абстрактно или конкретно понятие.

Н.С. Стандартът ISO/IEC 27001 дава ли някакво конкретно определение на понятието „сигурност"? То стана доста актуално в последните години...

Б.А. В самия стандарт дефиниция за "сигурност" няма и това е обяснимо. Винаги, когато се говори за сигурност, се има предвид някакъв конкретен аспект и се говори за "национална сигурност", "сигурност на работното място", "сигурност на доставките", "сигурност на информацията" и т.н. В ISO/IEC 27001"сигурност на информацията" е "запазване на поверителност, цялостност и наличност на информацията ..." В дефиницията е казано още, че могат също така да бъдат включени и други характеристики като автентичност, отчетност, неотхвърляне и надеждност. За прилагането на стандарта ISO/IEC 27001 е важно да се знае, че трябва да се вникне дълбоко в смисловото значение на термините и едва след това да се тръгва по пътя на разработване на система за управление на сигурността на информацията.
И още нещо ... Ефикасното прилагане на стандарта изисква познаване и на други, свързани с него поддържащи стандарти, един от които е ISO/IEC 27000, включващ всички термини.

Н.С. Какво определя повишения интерес към стандарта ISO/IEC 27001?
Б.А. Винаги, когато се появи нов международен стандарт, това може да се приема като реакция на възникнал глобален интерес. Така е и със стандарта за сигурност на информацията. Времето, в което живеем, наложи сигурността на информацията като неотменим императив за много и най-различни организации. Преди около двадесет години възникна интерес към качеството и така се появи популярният вече ISO 9001, последваха го ISO 14001 (за околна среда) и BS OHSAS 18001 (за безопасен труд). В наши дни, когато обществото ни като цяло е базирано на информационни технологии и когато станаха реални заплахите, които експлоатират тези технологии или заплахите, изразяващи се в опити за неоторизран достъп до данни, повечето организации нямат друг избор, освен да си създадат системно и планово построена защита на информационните си активи – не само в собствен интерес, но и в защита на интереса на своите клиенти, партньори, а и на обществото като цяло.

Н.С. Има ли международни стандарти за системи за управление и по отношение на другите аспекти на сигурността?
Б.А. Има. И всички те си приличат по това, че боравят с понятието "риск" и поставят изисквания за "управление на риска". ISO/IEC 27001 по същество е стандарт за управление на рисковете по отношение на сигурността на информацията.

Този документ е част от онлайн библиотеката на Алфа Куолити - www.alphaquality.org/bibl/bibl.html

Н.С. Според науката сигурността се прилага по отношение на четири вида активи – материални, финансови, хора и информация. ISO/IEC 27001 приложим ли е и за такива активи?

Б.А. Да, но стандартът не дава "стандартна" формула за видовете засегнати активи, а насочва организациите сами да определят кои са активите, които се нуждаят от защита. Така те може да се окажат различни за различни организации, но все пак вниманието е насочено към информационните активи – най-често информационни системи, сървърно, мрежово и крайно оборудване, преносими IT средства, бази данни и т.н. В частен случай "актив", който подлежи на защита, може да се окаже и определен човек – например, ръководителят на организацията, заедно с информационните и комуникационни средства, които той ползва, неговият автомобил (ако е оборудван с такива средства), че даже и бележникът му за записки и контакти, както и документи, които ползва. Работата по определяне на застрашените активи, а и ред други определящи действия при работа по СУСИ, е добре да се движи от добре синхронизиран и методически подкован екип от различни по профил специалисти. Иначе се оказва, че "техничарите" силно наблягат само на хардуерни и софтуерни средства за защита, "силоваците" пък наблягат на мерки и похвати, на които са ги учили и които са практикували в "силовите" ведомства и накрая идват "администраторите", които смятат, че всичко може да се постигне с издаване на заповеди и други действия по администриране.

Н.С. Какво дава на фирмите този стандарт – по-висока степен на сигурност или по-подредена система за управление? Или спокойствие, че са взели някакви мерки за сигурността си?

Б.А. Темата на този въпрос е за предимствата, които създава ефикасно действащата система за сигурност на информацията. Най-общото предимство е, че се намалява нивото на риска, изразено чрез намаляване на вероятността от инциденти и намаляване на тежестта на последствията от инциденти (ако настъпят), свързани със сигурността на информацията.

По-конкретно системата за управление на сигурността на информацията:

- създава и поддържа доверие сред клиенти, партньори, доставчици;
- предотвратява финансови загуби и поражения, причинени от изтичане на информация;
- опазва интелектуалния капитал и правата за интелектуална собственост;
- предпазва от загуба на пазарен дял;
- насочва вниманието към познаване и строго прилагане на законовите норми;
- защитава имиджа и репутацията на организацията;
- въздейства в посока "сигурност" върху всички свързани други организации и лица и така работи за изграждане на "верига на сигурността". Изисква от всички контрагенти да познават и прилагат отнасящи се за тях изисквания, както и приема техните изисквания;
- поддържа механизми за самопроверки и прилага подобрения;
- периодично "сканира" заплахите и насочва управлението на риска така, че да генерира адекватни и пропорционални мерки за защита;
- ползва поуките от своя и чуждия опит и създава подходящи превенции.

Връщайки се на зададения въпрос намираме повод да кажем, че няма никакъв смисъл да се подхожда формално и да се вземат "някакви мерки", които да осигурят само "спокойствие". Механизмите на стандарта, в частност оценяването на риска, дават възможност на организацията да оразмерява степента и видовете защита според текущото състояние на заплахите.

Н.С. Българите имат ли култура по отношение на защитата на информацията, според Вашите наблюдения от семинарите по този стандарт? Осъзнават ли значимостта на проблема „сигурност на информацията"?

Б.А. Мога да говоря за семинарите, които провежда консултантската фирма "Алфа Куолити Интернешънъл". На тези семинари при нас идват хора, които вече са осъзнали важността на проблема "сигурност на информацията" и искат да получат информация за изискванията на стандарта и начините за въвеждането им в практиката. Иначе, ако говорим за "българите" най-общо, то като че ли отново сме свидетели на забавена реакция или на някакво необяснимо изчакване. Това най-вече се отнася до фирмите, за които въвеждането на стандарта е въпрос на собствено решение на ръководството, тъй като и този стандарт, както и ISO 9001, не е задължителен. Но рано или по-късно и у нас пазарът ще си каже думата и фирмите, които се занимават с охрана и сигурност много скоро ще се конкурират и с това - дали са въвели, сертифицирали и поддържат система за сигурност на информацията. Например, ако клиент поиска да му бъде осигурена охрана или инсталирани технически системи за наблюдение, сигнализация и други подобни, той ще даде достъп до документация за обекта, ще допусне технически персонал за оглед и за монтаж и би искал да бъде напълно сигурен, че фирмата ще опази информацията за обекта и тя няма да стане достъпна за трети лица. Добра е реакцията на българския парламент, който през 2007 г. издаде Закона за електронното управление, но приложното му поле е ограничено само до административните органи, предоставящи административни услуги по електронен път и до обмена на електронни документи между такива органи. Законът засяга и дейността на лица, осъществяващи публични функции и организации, предоставящи обществени услуги.

Н.С. Какви клиенти търсят семинарите на тази тема – пострадали от загуба на информация или превантивно търсещи защита?

Б.А. Нямаме клиенти от типа "парен каша духа" или поне не знаем, защото няма как да разберем, дали сред клиентите ни има вече опарени. По-скоро това са представители на фирми, на които скоро им предстои да разработват системи. Те идват, за да си помогнат в разбирането и усвояването на стандарта, който, нека го кажем направо, ползва специфичен език и е нужно на семинарите да бъде превеждан "от български на български". Има и друга категория клиенти, които вече са запознати с ключови изисквания на стандарта, тъй като при тях има установена система за управление на качеството. Важно е да се подчертае, че една система за управление на качеството съгласно ISO 9001, ако вече е въведена и усвоена, помага много да се приложи ISO/IEC 27001 чрез допълнения към вече практикувани изисквания и интеграция на специфичните изисквания за управление на риска. Така ще се окаже, че тези, който имат системи за управление на качеството, вече са с една-две стъпки напред пред всички други.

Н.С. Имате ли обратна връзка за ползата и ефекта от ISO/IEC 27001 в практиката?

Б.А. В случаите, на които сме свидетели, хората сами си казват, че работата по усвояване на този стандарт им е отворила очите за много аспекти по сигурността на информацията, които те преди това или не са смятали за важни или не са ги знаели. Силата на стандарта ISO/IEC 27001 е в три неща. Първо, той включва Приложение А, в което има подробен, но все пак неизчерпателен, списък от мерки за защита, които трябва да бъдат прегледани дали са приложими и се прави подходящ за отделния случай избор. Второ, въвеждането на стандарта е подсигурено от фамилия други стандарти, съдържащи ценни пояснения и указания по прилагането му. И трето - ISO/IEC 27001 се въвежда като се вземат предвид решения и подсказки за добри практики по сигурността, дадени в стандарта ISO/IEC 27002. Нямаме силна и богата на данни обратна връзка, може би затова, защото става дума за чувствителна информация. Дали работи ефикасно една система за сигурност на информацията, само по себе си е информация, която не трябва да е достъпна дори и за консултанта, след като той приключи работата си. Вероятно като единствен и най-общ публичен критерий за успешно действаща система ще се окаже наличието или липсата на сведения за пробиви в сигурността – или както му казваме по нашенски – "издънка". Плюс това може да се добави и формален

Този документ е част от онлайн библиотеката на Алфа Куолити - www.alphaquality.org/bibl/bibl.html

критерий, изразяващ се в това дали системата е сертифицирана или не. Важно е да се знае, че системата за управление на сигурността на информацията не дава абсолютни гаранции за защита, но дава максимално близка до абсолютната гаранция при две условия – ако хората в организацията са разбрали, приели и следват установената политика за сигурност във всичките си практически действия и ако редовно се извършва щателно преоценяване на риска с всички, следващи оценката, действия за подобряване на практиката

Този документ е част от онлайн библиотеката на Алфа Куолити - www.alphaquality.org/bibl/bibl.html