# СИГУРНОСТ НА ИНФОРМАЦИЯТА "ИЗВЪН" IT СТРУКТУРИТЕ

(или "Сигурност на информацията за всички")

**инж. Бончо Антонов, Алфа Куолити**

Информационното общество е глобална, голяма и многолика общност, в която, освен големи и водещи, се причисляват и някои други фигури – по-"дребни" и разположени в периферията му, както те биха изглеждали от върховете на това общество. И в същото време те не са за подценяване, предвид на това, че твърде голямата част потребители на информационното общество са всъщност клиенти на неговите периферни части. Усилията, които полагаме в следващото тук изложение, имат за цел да разсеят някои, като че ли тръгнали да се утвърждават, заблуждения за "IT природата" на стандарта ISO/IEC 27001 и за да подкрепим тезата, че за "сигурност на информацията" може да се говори не само в организации с много добре развита IT инфраструктура, но и в приложното поле, където действа преобладаващото мнозинство на "периферните" участници със скромни ресурси.

За начало ще ни се наложи да си припомним текстове на самия стандарт.

Нека първо се спрем на наименованието на стандарта ...

| |
|---|
| "**Информационни технологии**. Методи за сигурност.<br>Системи за управление на сигурността на информацията. Изисквания" |

"Информационни технологии" има навсякъде и едва ли има бизнес, в който те да не се ползват. Тези технологии обслужват бизнеса, често без да са предмет на самия бизнес – т.е. организациите, които ги ползват, не са с IT профил. Такива организации може да са със съвсем скромно IT оборудване и да ползват най-обикновени IT технологии, но това не значи, че в съдържателно отношение информацията, с която работят, не предполага да бъде защитена. За всички тези случаи може да се каже така – няма пряка зависимост между степента на развитие на IT фактора, ценността на актива "информация" и нуждите от защита на информацията. Ето и пример – в някоя адвокатска кантора може да има само един или два локални персонални компютъра, евентуално свързани с Internet, ползващи електронна поща и нищо повече. Може да си представим колко чувствителна откъм характеристиката "поверителност" е информацията, с които работят адвокатите, колко уязвими понякога са информационните им активи и какви вреди носят заплахите.

Тезата ни намира допълнителна подкрепа и в следващите текстове на стандарта ...

| |
|---|
| 1 Обект и област на приложение |
| 1.1 Общи положения |
| Този международен стандарт се отнася за **всички видове организации**<br>(напр. търговски предприятия, правителствени агенции и организации с идеална цел). |

Може да отбележим, че това, което дават авторите на стандарта за пример, свързан с понятието "всички видове организации", е не само крайно лаконично, но и леко подвежда, защото не индуцира представи за широко и пъстро разнообразие.

и пак в стандарта, но малко по-нататък ...

| |
|---|
| Системата за управление на сигурността на информацията е предназначена, за да осигури избор на подходящи механизми за контрол по сигурността, които **да защитават информационните активи** и да дават увереност у заинтересованите страни. |

В тези, а дори и в други текстове на стандарта, няма и косвена подсказка, в която да се говори, че изискванията засягат само IT активи на организации със сериозен IT ресурс. Ако отидем в разсъжденията си в посока на противоположната крайност, то може да търсим прилагане на стандарта в организации, където "информационните активи" изобщо не са представени в IT формат. Може да предполагаме това поради чисто формални основания, ако се фокусираме в смисъла на дефинициите, които предлагат стандартите. "Актив" е "всяко нещо, което има стойност за организацията" (т. 3.1, ISO/IEC 27001), а "информация" е "значими данни". Стигаме до това, че "информационен актив" е "значими данни, които имат стойност за организацията". Така актив може да е и сбор от досиета на хартия.

Може да си помислим, че няма как да търсим прилагане на ISO/IEC 27001 в организация, в която няма информационни активи, подлежащи на защита, защото предназначението ѝ е да разпространява навсякъде информация, да има винаги гарантиран и безпроблемен достъп до информацията и без да има възможност потребителите на информация нарочно или неволно да нарушат цялостта на така разпространяваната информацията. Едва ли може да има точно такива случаи, освен не ако става дума за излъчване на ефирни програми от електронни медии. Но дори и в този случай сигурността на информацията може да бъде проблем, по-скоро вътрешен, защото персоналът, който прави подготовка за излъчване, може да допусне загубване, манипулиране или подмяна на информацията. Отделно от това, повреда или посегателство над оборудването за излъчване ще означава загуба на сигурността на информацията в характеристиката "наличност".

Няма да е прибързано, ако направим някои констатации:

- съдържанието на информацията и правата за достъп до нея не може да са единствени критерии за нуждата от защита. Тази защита може да обхване активи и технологии за подготовката и разпространението на общодостъпна информация;
- всеки един бизнес създава или ползва информация и части от нея, ако не цялата, трябва да са защитени, за да има сигурност в полза на клиентите и на други страни;
- дори бизнесът да ползва съвсем скромен IT ресурс, изискванията на ISO/IEC 27001 трябва да може да се прилагат, макар да се наложат твърде специфични, нетипични интерпретации за постигане на тези изисквания;
- има доста случаи, в които трябва да се осигури защита на "информационни активи", които изобщо не са с IT природа. Може тези активи да са в по-голяма степен критични и чувствителни, отколкото IT активите.

Всичко това може да изкажем като формално правило, че "Стандартът ISO/IEC 27001 не съдържа технологични предпоставки и ограничения към профила на организациите".

От такава позиция става ясно, че се налага да се работи с широк диапазон на подходящите интерпретации на стандарта, когато прилагането му ще става в неразвити IT структури, които обаче работят с чувствителни информационни активи, подлежащи на защита.

Ясно е, че не е възможно да се предлагат "рецепти" как да се подхожда при усвояване на стандарта в неразвитите IT структури, но може да опитаме да търсим акценти, които с голяма вероятност биха били подходящи.

Ето как може да изглеждат някои от акцентите.

**Подходящи принципи**
Системата за управление на сигурността на информацията трябва да стъпи на подходящо подбрани измежду известните принципи на сигурността. Ако IT ресурсът е слаб и особено, ако числеността на персонала е малка, тогава например принципът за "разделяне на задълженията" ще бъде или неподходящ, или нереализуем.

Започвайки проектирането на системата за управление на сигурността на информацията внимателно подбираме подходящи принципи и след това ги обявяваме, като документираме и смисъла, който влагаме в тяхното съдържание и който имат за конкретната практика.

**Добре обмислен и точно формулиран обхват**
Тук строго се придържаме към изискванията на ISO/IEC 27001, защото те задават какво точно да съдържа формулировката за обхват и граници на системата. Характеристиките на дейността описваме като сбор от процеси. Останалите елементи "местоположение", "активи" и "технологии" ги обвързваме пряко с вече декларираните процеси.

Проектирането на система ще обхване само процеси, за които поне една характеристика на сигурността има решаващо за процеса важност – поверителност, цялостност, наличност.

**Внимание при определяне на активите**
Лесно е да си представим, че една дори невзрачна на вид папка може да "има стойност за организацията" – т.е. да е актив – зависи какво съдържа! Малко по-трудно приемаме, че един човек може да знае много и важни неща и да се счита от системата за "актив", независимо че в дефиницията за актив се казва "всяко нещо, което ...", а не "всеки ...". От друга страна, ако в организацията има компютър, това не означава автоматично, че този компютър ще бъде актив, но може телефонът на секретарката на шефа да е "актив". Ако организациите с развита IT структура могат, без грешка, веднага да си определят активите и собствениците, тези, които имат скромен ICT ресурс, е по-добре да не бързат.

Тръгваме от интересите и изискванията на законите, страните по договор и клиентите. От тази позиция разсъждаваме за процесите и дейностите, чрез които ги постигаме и си правим сметка за активите, участващи или осигуряващи такива процеси и дейности. Важна следваща стъпка е да установим точно уязвимостите на определените активи.

**Добро познаване на рисковете**
Доброто познаване на рисковете, пред които е изправена организацията, е необходимо, за да се намери точната мяра на ресурси и мерки за защита, необходими за постигане на сигурност. Смята се, че почти всяка организация трябва да разглежда заплахи, които са от физически характер, загуба на данни, неизпълнение на законови норми, недостъпни данни, необходими за работата и заплахи, свързани с ползване на мобилно оборудване. Доброто познаване на рисковете е необходимо, за да се намерят решения за сигурността, съобразени с това – колко средства биха могли да се отделят за защита и какви загуби може да си позволи организацията, ако бъде нарушена сигурността.

Доброто познаване на рисковете означава:
- систематично търсим информация за заплахи и за източници на заплахи;
- не неглижираме заплахите – които сме понасяли преди и които реално очакваме;
- не изпадаме в параноична треска всеки мейл да е заплаха и всеки човек – шпионин;

- знаем, че всяка защита, дори и най-добрата, може да бъде разбита и си правим сметка за наличните и достъпни ресурси, за да ги насочим към критичните заплахи и за да определим по-реалистично дълбочината на защитите;
- ползваме подходяща методика за оценяване на рисковете;
- оценяването на рисковете, освен вероятност и последици, включва още и елемент, които отразява дали е лесно или по-трудно да се установи наличието на заплаха.

**Нива на оценяване на рисковете**
Те може да са две – оценяване "на високо ниво" и "оценяване в детайли". На високо ниво се оценяват заплахите, въздействията върху активите и рисковете, отнесени към онези от активите, от които в най-голяма степен зависят бизнес процесите. Навлизане в детайли означава оценяването да се насочи точно – или към информационна система (например, става дума за хотел или пък за спедиторска фирма) или към рисковете, свързани с човешкия фактор (за фирма, която проектира и инсталира системи за наблюдение и охрана), или към рисковете за отклонение от правни норми (ако бизнесът в значителна степен е определен от такива норми – адвокатска или митническа кантора), или към физически аспекти на сигурността (ако средата, в която работи организацията, съдържа такъв вид уязвимости – например, офисът на фирмата се намира в квартал, известен на полицията с многобройни случаи на кражби). Накратко – оценяването в детайли ще отрази спецификите на бизнеса и неговите уязвимости и така ще допълва оценяването на високо ниво. Наред с това оценяването ще даде основа за разработване на най-необходимите за една конкретна практика политики и процедури.

Търсим най-подходящото, според реалностите, съчетание на двете нива на оценяване.

**Метрични скали, ползвани при оценяване на рсковете**
И те обикновено са две – количествена (която ползва числови стойности) и качествена (която ползва нива на градация). Ползването на количествените мерки често налага да се стъпи на обеми от данни за минал период или да ползваме статистическа информация (например, данни за надежността на техническо оборудване). При тях има затруднения и по–силно изразен субективизъм, ако се прилагат за някои категории рискове, каквито са от загубата на реноме или от хакерска атака. Качествените мерки са сред по-широко прилаганите и имат предимството да служат добре дори в условията на една по-голяма неопределеност. Методиките за оценка на рисковете, които ползват качествени скали, ще се окажат по-подходящи и по-прости за случаи на слабо развити IT инфраструктури.

**Комбинирано документиране**
По-полезна и по-работоспособна за организация със скромен IT ресурс ще се окаже тази система, която е по-пестеливо и по-просто документирана. Многословните и усложнени правила и изисквания, сами по себе си са вътрешна заплаха за сигурността.

Полезно е да се минимизира като съдържание документалния комплект на системата и да се търсят кратки и прецизни формулировки на изискванията. Не е грешка да се ползва опцията, дадена от ISO 9001, изискванията за няколко процедури да се групират в тяло на един документ и така да се получи т.нар. "съставна" или "макро" процедура.

**Приложение А на ISO/IEC 27001 – средство за обвързване на системата с реалността**
Освен коментираните по-горе, със сигурност ще има и други елементи на стандарта и на практиката, за които ще се наложат по-различни интерпретации и подходи. Те може да

бъдат разглеждани по-внимателно и по друг повод, защото тук се ограничаваме само до това да бъде представена и защитена тезата "*сигурност на информацията за всички"*.

Тук по-важно е да коментираме целите по контрола и механизмите за контрол, дадени в Приложение А на ISO/IEC 27001, тъй като там очакваме да се проявят по-голямата свобода и по-пъстрото разнообразие от интерпретации, отколкото при анализирането на основните изисквания на стандарта, дадени в раздели 4, 5, 6, 7 и 8. При това, знаем, единствено раздели 4 и 5 съдържат изцяло свързани с управление на сигурността норми. В разделите 6, 7 и 8-ми изискванията са най-близки до ISO 9001, което улеснява организациите със СУК.

Ще се наложи за последен път да вземем цитат от стандарта, този път - от Приложение А

| Приложение А |
| --- |
| (основно) |
| ЦЕЛИ ПО КОНТРОЛА И МЕХАНИЗМИ ЗА КОНТРОЛ |
| Целите по контрола и механизмите за контрол, описани в таблица А.1, са заимствани от ISO/IEC 17799:2005 и са в съответствие с точки от 5 до 15. **Списъците в таблица А.1 не са изчерпателни и организацията може да счете, че са необходими и допълнителни цели по контрола и механизми за контрол.** |

Изборът на цели по контрола и механизми за контрол следва получената оценка на рисковете с прилагане на критерии за допустимост. Тук именно организациите със слаба IT инфраструктура би трябвало да проявят реализъм, смелост, въображение и гъвкавост, за да се възползват от трите свободи, които стандартът предлага:

- да се усвоят избраните цели и механизми по подходящи за организацията начин и обем;
- мотивирано да се обявят за изключени неприложимите цели и механизми;
- да се добавят свои цели и механизми, такива, каквито ги няма в Приложение А, но се преценява, че са смислени и необходими от гл. т. на практиката.

Оказва се, че има и четвърта свобода на действие, за която стандартът не споменава, но нейният смисъл ясно се чете между редовете на Приложение А. На база на комбинация на горните свободи имаме възможност да направим и субституция (т.е. заместване) на цел и механизми за контрол. Това ще е подходящо в случай на цели и механизми, които са в голяма степен, но не категорично и не изцяло неприложими и затова не ги изключваме, а ги преформулираме и приближаваме до практиката си, за да станат ползваеми.

Добре би било постановката *"сигурност на информацията за всички"* да бъде по–широко разпространена и добре разбрана, за да се разсее мита за IT природата на стандарта и за IT инфраструктурата като доминиращ актив и критерий за прилагане на ISO/IEC 27001.

Какви ползи се постигат, ако тази постановка бъде наистина усвоена?

- консултантите ще имат по-адекватни и приспособими към клиентите им решения;
- одиторите от трета страна няма да извиват ръцете на клиентите, търсейки буквално и формално съответствие единствено чрез решения, типични за големи IT фирми;
- повече организации ще искат да ползват ISO/IEC 27001, за да гарантират сигурност;
- печелим всички ние, които постоянно и неизбежно имаме отношения със субекти на информационното общество и искаме при това да получаваме и сигурност.

Най-важна е ползата, която могат да имат онези организации, които преди това въобще не са имали идея да посегнат към стандарта ISO/IEC 27001, поради ниско IT самочувствие