АКЦЕНТИ ПРИ РАЗРАБОТВАНЕ, ВНЕДРЯВАНЕ, ОДИТ И СЕРТИФИКАЦИЯ НА СИСТЕМИТЕ ЗА УПРАВЛЕНИЕ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Бончо Антонов, старши консултант в "Алфа Куолити Интернешънъл"
Мария Нанкова, представител на "AENOR Internacional" в България

Доклад пред Националната конференция по качеството, ноември 2009 г.

БАНАЛНИ ИСТИНИ И ФАКТИ ЗА СИГУРНОСТТА НА ИНФОРМАЦИЯТА

Понятието "сигурност на информацията" ...

CIA – това не само са популярните инициали на ЦРУ, а са и абревиатура на трите основни характеристики на информационната сигурност:

C – confidentiality (поверителност)
I – integrity (цялостност)
A – availability (наличност)

Сигурност на информацията – това е състоянието на неделимост и трайно запазване на тези характеристики в информационната и обща практика.

Иначе казано, сигурност на информацията има, когато едновременно:

- информацията не се разкрива и не е достъпна за неупълномощени;
- свързаните с информацията активи са комплектни и опазвани;
- при заявка от оторизирано лице информацията е винаги достъпна.

Сигурността на информацията се отнася за широк кръг организации

У нас Законът за електронното управление задължава определени организации да разработят и поддържат системи за управление на сигурността на информацията. За останалите организации въвеждането на такива системи е доброволно и така обществото е оставено да разчита на тяхната преценка за необходимостта да създадат и поддържат сигурност на информацията.

Коловозите на българския манталитет ни карат да мислим, че докато не стане някъде някоя голяма издънка, "доброволното" не се смята за необходимо. За да не звучи като "консултантски рекет", тук няма да посочим видовете фирми и сектори, в които сигурността е елемент на качеството и е *"conditio sine qua non"*.

Сигурността на информацията е критична за бизнеса

От лошо общо управление една фирма може да фалира или може да се компрометира след година и повече. От изтичане на информация, пробиви в сигурността или невъзстановимо прекъсване на обслужването, организацията може да се срути само за една нощ, без да може да се възстанови отново и без

изобщо да отчитаме тежките последици, които ще понесат нейните клиенти, другите заинтересовани от организацията страни, а понякога и цялото общество.

Сигурност е необходима за информацията във всичките й форми

От гледна точка на сигурността на информацията, пораженията от атака върху достъпа до информация може да бъдат от един порядък, независимо дали някой неправомерно е бръкнал в база данни или е успял да надникне в папка.

Всяка от характеристиките на сигурността трябва да бъде постигната и поддържана, независимо как се ползва информацията – в компютър или мрежа, в медийна среда, в писмен вид, в комуникация, като разговор или друг начин.

Информацията изкушава

Резултати от проучвания (не в България!) показват, че служителите са склонни да мислят, че постигат лична сигурност като присвояват, укриват или задържат информация. Това се отнася и до фирмите – не са малко тези, които не биха отказали да се доберат до данни за преките си конкуренти. Някои дори са готови и да плащат, за да им се достави чужда информация “по заявка”.

БАНАЛНИТЕ ОПАСНОСТИ ПРИ СИСТЕМИТЕ ЗА СИГУРНОСТ

Движение по утъпкани пътеки

Неудържимият юруш да се правят системи за управление на качеството, околната среда и безопасен труд “от днес за утре”, заради търгове и конкурси, утъпка късите пътечки, по които фирмите някакси “тайно и полека” от “гола поляна” стигат до чисто формалните признания на органите за сертификация, че имат действащи системи и че те заслужават сертификат, съпоставим с тези, които се издават по света на организации, изкачили върха с усилия. Остава въпрос дали такива фирми ще спечелят и неформалните признания на своите клиенти и засегнати страни – единствен верен критерий за ефикасно действащи системи.

Светкавичните разработки на системи за управление на сигурността на информацията ще произведат резултати, достойни за категория “бързата кучка”. Тази опасност е съвсем реална – твърде много фирми проспиват да осъзнаят необходимостта от управление на сигурността със системни средства и когато условието “сигурност” за сключване на договор им опре в ребрата, се задействат.

Системите за управление на сигурността на информацията са по природа уникални във всяка организация и се създават в среда на обективност и реализъм.

Сигурност и мениджмънт

Управлението на сигурността на информацията е присъща част на общия мениджмънт. Грешка е то да се възложи на IT структурно звено, а ръководството и всички останали звена да са в позицията на “потребители” на сигурността.

Всяко друго нещо би могло, но рискът е онова, което никой мениджър не трябва да пренебрегва, освен само ако е решил да си поиграе на мениджмънт.

Срещу асиметричните подходи

Асиметричните подходи са непълноценни и деформират системите за сигурност. Става дума, че се забелязват практики при въвеждането на системи, в които водещи специалисти дебалансират системите с много силен уклон към ограниченото поле на тяхната компетентност:

- IT специалистите наблягат силно само на техническите и програмните мерки и средства за защита, едва ли не отричайки всички останали;
- тези, които са станали специалистите в средите на МНО, МВР или са със стаж в други по-особени структури, насочват работите към мерки и средства по физическа и техническа защита, към мерки по отношение на персонала и други мерки – понякога специфични, че даже и екзотични;
- специалистите, станали “царе” на познатите системи за управление - качество, околна среда и безопасен труд, наблягат едностранно само на общото (то го има!) между тези стандарти, но това става за сметка на непълно развити специфични за стандартите за сигурност изисквания.

Стандартът ISO/IEC 27001 е замислен и реализиран така, че ни насочва към точно балансирана и изчерпателна композиция от аспекти, мерки и средства за защита, в рамка на общ системен подход към сигурността. Всяка система за сигурност, реализирана със залитане в една или друга посока, наподобява паун, който е разперил половината си опашка – отстрани той изглежда като оскубан.

Интернет – вредата от търсачките

Не търсете в Интернет безплатни копия (руски, австралийски и други) на стандартите. Купете си официалните им издания и ползвайте само тях.

АКЦЕНТИ ПРИ ПРОЕКТИРАНЕТО И ВНЕДРЯВАНЕТО НА СИСТЕМИТЕ

Силни връзки на стандарта с неговата фамилия

Ако сега се случва СУК да се въвеждат и сертифицират само въз основа на стандарта ISO 9001, то въвеждане на ефикасна система за сигурността на информацията само по изискванията на ISO/IEC 27001 не е достатъчно.

ISO/IEC 27001 също принадлежи на фамилия стандарти, но връзката му с част от тях е критично важна в ситуации на проектиране и внедряване на система:

- ISO/IEC 27000 – общ преглед и речник;

- ISO/IEC 27002 – добри практики;
- ISO/IEC 27003 – указания за внедряване;
- ISO/IEC 27004 – измервания;
- ISO/IEC 27005 – управление на риска.

Отделно, фамилия 27000 е свързана и с други поддържащи стандарти на ITU, ISO/IEC и BSI, като в отделни случаи връзката и с тях е много важна:

- справяне с инциденти;
- възстановяване след бедствия;
- сигурност в IT мрежите;
- използване на доверени трети страни;
- системи за разкриване на намеса.

Особено интересни и важни са ръководствата на BSI от серията BIP:

- BIP 0071 – по изискванията и по добрите практики за сигурност;
- BIP 0072 – по проверка на готовността за одит на СУСИ;
- BIP 0073 – по внедряване и одит на мерките за сигурност (контроли);
- BIP 0071 – по измерване на ефикасността на СУСИ.

“Верига на сигурността”

Концепция за “верига на сигурността” не е обявена изрично, но се вижда ясно между редовете на стандарта. По подобие на другите стандарти за системи за управление на “риска”, и тук се разбира това, че не може да се постигне ефикасна сигурност, ако целите, мерките и средствата бъдат ограничени само в рамките на организацията. Те трябва да засегнат нейните доставчици, партньори и други външни страни, които са участници в бизнеса, или да се иска тези страни също да въведат свои системи.

По подобие на другите системи, във “веригата на сигурността” е добре да има редовен обмен на информация на експертно ниво. Интересното тук е, че веригата на сигурността може да включи не само преките бизнес-партньори, но и други външни страни – експерти в различни области и аспекти на сигурността.

Профил на риска – компоненти

Организацията трябва да познава отнасящите се до нея рискове. Това е важно за точното насочване на ресурсите, нужни за управление на рисковете.

Профилът на риска трябва да включи най-малко следните компоненти:

- правна рамка;
- организационна основа;
- информация и IT системи;
- бизнес процеси, в т.ч. аутсорсинг, доставки, клиенти;
- въздействия на външната среда.

Изработването на “профил на риска” помага да се изясни изпълнението на анализа на риска като “систематично използване на информация с цел да се идентифицират източниците и да се прецени рискът”.

Профилът може да бъде общ и разширен и това пряко кореспондира с различните нивата на подробност при оценката на риска

Обхват на СУСИ и интерфейси

Обхватът на СУСИ, както и да бъде определен, не трябва да изключва:

- персонала, участващ в дейности на системата;
- процесите и услугите;
- информацията и информационните системи;
- политиките, процедурите и документацията;
- интерфейсите и връзките на системата;
- поддържащата ICT инфраструктура;
- физическото разположение.

При определен обхват, вниманието следва да се насочи към определяне на външните и вътрешни интерфейси – места, през които заплахите атакуват. Управлението и контролът на информацията през тези интерфейси в голяма степен осигуряват защитата на бизнеса. Средствата за управление и контрол – те обикновено са договори и споразумения за услугата, както и оперативни процедури, инструкции и наръчници.

Степенуване на решенията за управление на риска

Подходът за степенуване на решенията за управление на риска осигурява добра съвместимост на системата за управление на риска със стратегическите и икономически цели на организацията. Степенуването на решенията се очаква да преминава последователно през отделни фази в зависимост от предпочитанията:

- избягване на риска;
- прехвърляне на риска върху външна страна;
- намаляване на риска;
- съзнателно възприемане на риска.

Схемата за степенуване не се прилага буквално и автоматично, защото се оказва, че сигурността на информацията има цена, която е в ползите, които трябва да бъдат пожертвани. Във всяка фаза има момент на преценка дали подобрената сигурност ще е по-подходяща от определените бизнес ползи, ако рискът бъде съзнателно възприет. Освен това се налага да се мисли и по въпроса дали прилагането на защитни мерки за намаляване на риска не крие опасност от други по характер неблагоприятни последици. Обичайна практика е малките рискове да бъдат възприемани, но и това също изисква преценка, защото може да подведе – малкото за една организация, за друга може да не е.

ОДИТ НА СИСТЕМИТЕ ЗА СИГУРНОСТ

За да бъде успешно сертифицирана една СУСИ тя трябва да отговаря на раздели от 4 до 8 на стандарта. Основни доказателства за спазване на тези изисквания се очаква да има в съответните документи и записи за планирани, изпълнявани и осъществени дейности, като тези от следната таблица

Раздели на стандарт ISO/IEC 27001	Документ-доказателство
4.1 Общи положения	Политика по сигурността
4.2 Създаване и управление на СУСИ	
4.2.1 Създаване на СУСИ	Политика по сигурността Списък на активите Анализ на рисковете Управление на рисковете Документ за приложимост
4.2.2 Внедряване и функциониране на СУСИ	План за сигурност
4.2.3 Наблюдение и преглед на СУСИ	Управление на инциденти Вътрешни одити Преглед от ръководството Наблюдение на целите
4.2.4 Поддържане и подобряване на СУСИ	Действия за подобряване Превантивни и коригиращи действия
4.3 Изисквания към документацията	
4.3.1 Общи положения	Политика по сигурността Цели по сигурността Процедури Анализ на рисковете Управление на рисковете Записи Документи за приложимост
4.3.2 Управление на документите	Процедура за управление на документите
4.3.3 Управление на записите	Процедура за управление на записите
5 Отговорност на ръководството	
5.1 Ангажимент на ръководството	Подписани политика и планове Подписани критерии за допускане на рискове Преглед, одобрен от ръководството
5.2 Управление на ресурсите	
5.2.1 Осигуряване на ресурси	Планове за сигурност
5.2.2 Обучение, осъзнаване и компетентност	Планове за обучение Записи от обучение
6 Вътрешни одити на СУСИ	План за одити Доклади от одити
7 Преглед от ръководството на СУСИ	Доклад от преглед от ръковоството
7.1 Общи положения	
7.2 Входни елементи за прегледа	

7.3 Изходни елементи от прегледа	
8 Подобряване на СУСИ	
8.1 Непрекъснато подобряване	Записи за действия за подобряване
8.2 Коригиращи действия	Записи за коригиращи действия
8.3 Превантивни действия	Записи за превантивни действия

СЕРТИФИКАЦИЯ

Сертифицирането на система за управление представлява „получаване на документ", който признава и удостоверява наличието и функционирането на система съобразно изисквания, залегнали в стандарт за съответния вид системи. Издаването на сертификат за спазване на стандарт се осъществява единствено от организации, които са надлежно акредитирани от орган, който е определил критерии за осъществяване на дейностите по сертификация (напр. в България това е ИА „Българска служба по акредитация").

Сертификацията на системи за управление на сигурността на информацията се извършва спрямо изискванията на ISO/IEC 27001. ISO/IEC 27002, споменат в горните редове, не е стандарт, по който се сертифицира, но се препоръчва използването му като ръководство за добри практики.

Ясно е, че предметът на сертификацията не е изрично сигурността на информацията в организациите, а е системата, чрез която тази сигурност бива управлявана.

Предимствата, които дава сертификацията на СУСИ са:

- създава имидж и работи за репутацията организацията;
- дава тласък на работите по опазване на информацията;
- генерира доверие пред трети лица и доказва стриктно управление;
- представлява фактор, отличаващ организацията от конкурентите ѝ;
- ако не съществува друга система за управление, създава култура на процесен подход и на непрекъснато подобряване, което се отразява положително на цялата структура.

Организация, която желае да ѝ бъде издаден сертификат, трябва да се свърже с акредитиран орган по сертификация (сертификатор).

Сертификаторът изисква основна информация за предприятието, като например вид стопанска дейност, брой на заетите и дейности, които ще бъдат сертифицирани, за да подбере подходящ екип от одитори и да определи броя дни, необходими за одит. Обхватът на СУСИ или видовете дейности, за които се отнася, се определя от организацията, тъй като не е необходимо системата да се отнася за всички звена. Обичайно е обхватът на СУСИ да се ограничи до онези услуги, отдели или процеси, за които е най-просто и/или за които е най-важно да се въведе, било защото усилията са по-малко или защото отзвукът от проекта (вътре или извън предприятието) е по-значим. Одитът е в два етапа

Етап 1: Преглед на документацията

Одиторският екип преглежда документите на СУСИ, за да провери дали съответстват на основните изисквания на стандарта и подготвя доклад с констатации. Ако бъдат открити сериозни отклонения от изискванията на стандарта, се информира предприятието-кандидат за невъзможността да бъде сертифицирана системата в съществуващите условия. Ако отклоненията са малки, то те трябва да бъдат отстранени преди следващия етап, който се провежда обикновено месец по-късно.

Етап 2: Сертификационен одит.

Одиторският екип търси и набира обективни доказателства за изпълнение както на изискванията на стандарта, така и на собствените политика, цели и процедури на СУСИ. Ако не се установят сериозни несъответствия, следва процедурен ред, при който на организацията се издава сертификат.

ЗАКЛЮЧЕНИЕ

За доклад, който започва с банални истини, не подхожда да има банално заключение. В един от романите на Жюл Верн се разказва за непримиримия дуел на двама велики асове във военната техника – единият създавал все по-непробиваеми брони, а другият ги атакувал с все по-мощни снаряди. Историята им приключва с това, че двамата стискат ръце и обединяват знанията си, за да стане възможно да се изстреля снаряд с екипаж към луната. В днешните ни глобализирани времена, в които информацията е толкова насъщна и толкова навсякъде необходима, за съжаление, все още няма място за такъв поетичен хепиенд. Вече няма човек, който да отрече, че сигурността във всичките й аспекти е неотменно изискване в ежедневието. А сигурността на информацията в полето на бизнеса е толкова необходима, колкото е немислим самият бизнес без ползване на информация. Информацията все още е толкова беззащитна, че прави апетита на “злите сили” все по-изострен и коварен. Редки изключения са случаите, в които най-печените хакери се покръстват в права вяра и слагат на жертвения олтар на сигурността уменията си в полза на обществото и бизнеса. Накрая трябва да изплюем камъчето – няма и не може въобще да има система за сигурност, която да опазва винаги и от всичко активите на организацията, колкото и добре да е разработена и да е в пълно съответствие с ISO/IEC 27001. Ще се появяват винаги нови заплахи и нови уязвимости, ще стават събития и инциденти по сигурността, но те вече ще бъдат прихванати от добре изпипан подход за предотвратяване или минимизиране на лошите последици. Самите автори на стандарта казват, че не е толкова важно да се проектира, внедри и сертифицира една система, колкото да се осигури нейното поддържане и развитие, чрез периодично оценяване на риска и чрез прилагане на механизми за подобрения. Там, където сигурността е особено важна, силовите структури на обществото влизат в действие и не допускат компромиси. По подобен начин в организациите, така си мислим, силовите похвати на мениджмънта трябва да бъдат упражнени в цялата им строгост, когато трябва да се внедрява, поддържа и подобрява система за управление на сигурността на информацията – за да има бъдеще за бизнеса и спокойствие и ползи за неговите клиенти