Технически университет – София

ПГ по Компютърни Технологии и Системи - Правец

Упражнение - 5

СИСТЕМИ ЗА СИГУРНОСТ

Тема: Прилагане на процедури за сертификация

Изготвил:

Доц. д-р Румен Трифонов

1. Общи положения при процеса по сертификация

1.1. Дефиниция и класификация

Терминът сертификация (certification) се отнася за потвърждаването на определени характеристики на обект, лице или организация. Това потвърждаване често, но не винаги, е осигурено чрез някаква форма на външен преглед, проучване, оценяване или одит. Акредитацията (официалното признаване) е процес на сертификация на специфична организация. Това е универсален инструмент в световната практика за постигане на сертифицирана информационната сигурност. Дефиницията за сертификация на Международната организация по стандартизация (ISO - International Organization for Standardization) е: „Сертификацията е процедура, чрез която трета страна дава писмено уверение за това че продукт, процес или услуга отговарят на специфични изисквания". Други ISO дефиниции: „Сертификационното тяло е орган, доверен на един или повече потребители, за създаване и назначаване на сертификати“; „Акредитацията е процедура, чрез която авторитетен орган дава официално признание за това, че организация или лице са компетентни да изпълняват специфични задачи“.

Важно е за всеки сертификат по информационната сигурност ясно да описва какво означава. Сертификатът трябва да описва как е от значение за дейностите, които се извършват. Ако обхвата на схемата за сертифициране е твърде тясен, то тогава получаването на сертификат може да е лесно, но той вероятно не би бил приложим за всички дейности, които се извършват. Ако схемата обхваща всички възможни аспекти, тогава процедурата по оценка може да бъде или твърде лесна за преминаване, или действително трудно някой ще се сдобие със сертификат.

Една добра схема за сертификация намира разумен баланс между ресурсите, които трябва да бъдат инвестирани и ползите, които могат да бъдат добити. За да се постигне това, първоначалните изисквания към

сертификационната схема са тя да бъде организирана, ясно написана и определена. Проблемът, обаче, често се крие в тълкуването на изискванията за сертифициране от страна на изпълнителите, както и в прилагането и използването на полученият сертифициран елемент от организацията.

Сертификатът е резултат от успешното приключване на процедура, преценяваща дали определена професионална дейност действително отговаря на набор от изисквания. Изискванията могат да бъдат определени от стандарт, или могат да бъдат избрани без позоваване на който и да е стандарт. Сертификатът дава информация на потенциалния клиент (например клиент на ниво на сигурност), прикрепен към продукта или услугата, която той купува, и улеснява сравнението между продуктите или услугите от различни видове или марки. Колкото по-признат и разпространен е един сертификат, толкова по-ценна е информацията, която той предоставя и толкова по-лесно е сравнението между продукти и услуги.

Започването на сертификционен процес изисква бъдещият притежател на сертификат да обясни и документира способностите и да оцени слаботите, въз основа на информация от схемата за сертификация. Подходящо проектираните сертификационни схеми могат също да помогнат за използването и конфигурирането на продукт или услуга по сигурен и законосъобразен начин (защото подобна конфигурация трябва да бъде разработена по време на процеса по сертификация. Организациите дори могат да следват принципите на сертификационна схема без всъщност да получат сертификата. Схемите за сертификация също подобряват сигурността, защото те са стимул за подобрение, тъй като компании и физически лица се стремят към репутацията, свързана със сертификата.

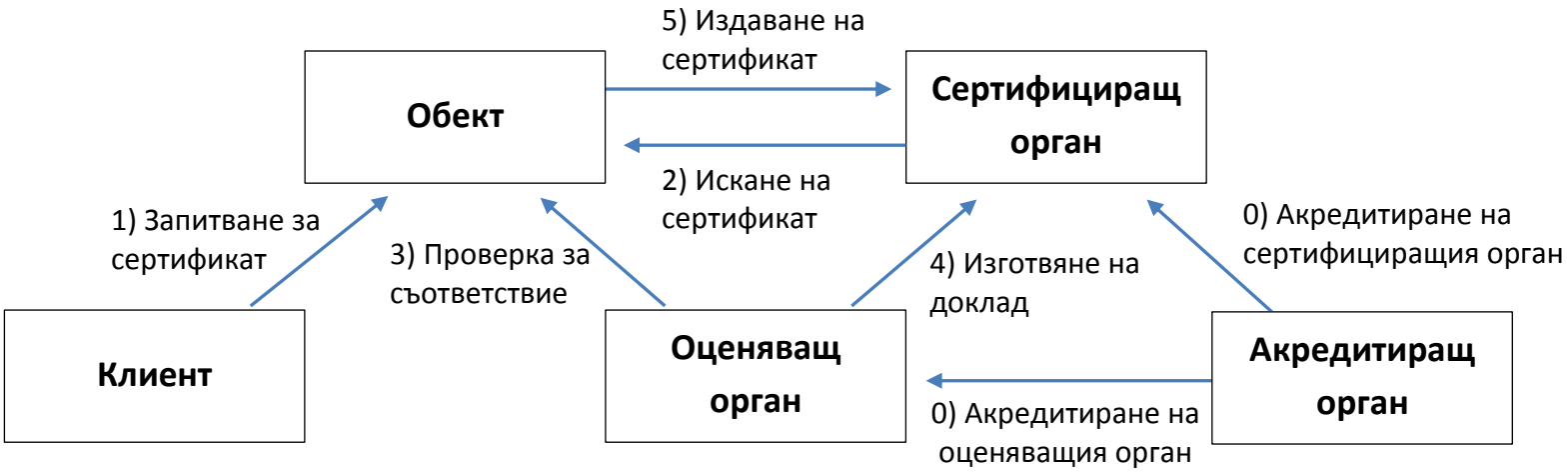
Ценността на сертификацията зависи от контекста, в който тя ще бъде използвана и може да се променя с течение на времето. В идеалния случай организациите ще разработят процес около избора и използването на сертификации. Това може да включва идентифицирането на подлежащи на сертификация процеси, хора или продукти, определянето

на цели, изборът на подходяща схема, управлението на оценяването и преоценяването, преглед за това дали сертифицирането отговаря на целите и накрая възможност за спиране използването на определена схема.

1.2. Създаване на йерархията на доверие

За да получи сертификат, обекта (хора, процес, продукт) трябва да премине през оценяване. Трета страна проверява дали обекта спазва стандарт или определен набор от правила. Ако обекта премине тази проверка, сертификата бива издаден. В някои случаи придобиването на сертификат по информационна сигурност е толкова лесно.

За да получи признание от страна на правителството, сертифициращия орган трябва да бъде „акредитиран“. Много организации за сертифициране на продукт са акредитирани според Европейския стандарт (European Standard) EN 45011. Тези европейски изисквания EN 45011 към сертифициращите органи са много важни. Те гарантират отсъствието на комерсиален търговски интерес при дейността по сертифициране. В някои случаи правителството може също така директно да упълномощи дадена организация с право за определен тип сертификат, като лабораториите по оценяване, участващи в процеса по сертифициране са акредитирани в съответствие с ISO 17025.



Сертификационните схеми осигуряват работна рамка за издаване на сертификати. Това обикновено включва обхват, правила за оценяване и също така аспекти за подновяване. Много е важно да бъде прецизно описан обхвата на обекта, който ще бъде сертифициран („обект на оценяване“ – target of evaluation), и това да стане в началото на процеса.

Съответствието с дадена сертификационна схема може да бъде оценено по различни начини: с изпит/ тест/ контролен списък, партньорска проверка или с формален анализ. Въпреки че експертите имат различни мнения относно кой е най-подходящия метод, изглежда има някакво споразумение за това, че сертифицирането на хора се нуждае от „меки“ критерии, докато сертфицирането на организации и продукти се нуждае от „твърди“ критерии.

За хора, изпитването се счита за основна форма на оценяване, а за по-напреднала форма на оценяване е необходима партньорска проверка (въпреки че някои твърдят, че партньорската проверка е уязвима заради възможни „близки отношения“).

За продукти и организации е необходим анализ от независима трета страна, който често се фокусира върху развитието или операционните процеси.

Въпреки това, анализът от трета страна може да работи само ако няма никаква полза за оценителя и просто да угоди на клиента, или ако на мястото има механизъм за наблюдение.

1.3. Примерно протичане на сертификация

Общо протичане на една сертификация:

Сертификационния орган представя оферта на базата на клиентските данни, като например брой на служителите, брой на филиалите и обхват на процесите. От тях се съставя оферта, в която се документират необходимите човеко-дни одит.

Клиента възлага изпълнението и съобщава желана дата за провеждане на одита.

Сертификационния орган потвърждава възлагането и се сключва договор, който има същата продължителност като на сертификата.

След това той възлага на одиторския екип/ одитора и потвърждава на клиента датата на одита.

В един определен срок клиента изпраща на одитора неговата система за управление. Тази проверка на документацията се извършва само при сертификационния одит.

Водещият одитор решава относно пригодността на документацията и подготвя съответния доклад. При съответствие, той препоръчва провеждането на сертификационния одит. Ако намери отклонения, моли за корекции.

След проверка на документацията и на база на възлагателната поръчка, водещият одитор подготвя плана за одит и го предоставя на клиента.

Провежда се одита. За начало на един сертификационен период се счита сертификационния одит, който продължава годишно с инспекционните одити.

Водещият одитор изготвя доклада за одит и изказва препоръка.
Тя може да бъде:

- Даване/запазване на сертификата;
- Даване/запазване на сертификата след приключване на коригиращите мероприятия;
- Последващ одит;
- Прекъсване на сертификационния процес;

Коригиращите мероприятия трябва да се приключат в рамките на 90 дни. След проверката и одобрението на водещия одитор към доклада от одита се прилагат съответните документи.

Сертифициращата организация проверява дали одита е бил правилно проведен, дали всички документи за одита са налични и дали съдържанието на тези документи отговоря на правилата. Тя предоставя и сертификата. Своевременно, преди следващия одит, се определя съвместно датата на му.

Ако предстои ресертификация, сертифициращият орган изготвя оферта на базата на актуалните данни на клиента.

1.4. Предимства на сертифицирането

Сертифицирането означава неизбежно подчинение на определени правила. Когато тези правила наистина се спазват, те дават много предимства. Доказано увеличават печалбата, както и постигат по-висока удовлетвореност на клиента, също и посредством избягването на грешки, вместо увеличаването им.

- Един сертификат е рекламно средство;
- Един сертификат увеличава репутацията и външното влияние;
- Една сертификация съдейства за постигане на целите;
- Ориентацията към клиента се усилва;
- Вкарва се непрекъснато подобрение;

- Насърчава се разширяването на компетентността на служителите;
- Служителите по-бързо и ефективно навлизат в работата;
- Развитието на доставчиците подобрява качеството на доставките.

2. Сертификация на информационната сигурност

2.1. Сертификация на хора

Има много схеми за сертифициране на физически лица за информационната сигурност. Повечето от тях се издават от частни организации, следвайки повече или по-малко задълбочено оценяване на възможностите на лицето в информационната сигурност. Някои сертификати се издават от доставчици на продукти за сигурност, основно сертифициращи това, че лицето е в състояние да работи с определен продукт.

В повечето случаи, сертификацията на дадено лице се отнася до специфични знания в областта на информационната сигурност. Рядко човек може да получи академично признание на професионалист по информационна сигурност. Това е в разлика с медицината например, където човек бива оценен и накрая удостоен с докторска титла, която му позволява да работи в медицинската професия. Тази професия е регламентирана от закона и ръководена от акредитирани органи. Повечето схеми за сертификация на информационната сигурност нямат този официален мандат, въпреки че някои са акредитирани по Международен стандарт ISO / IEC 17024:2003.

Този стандарт хармонизира процеса за сертификация на хора като определен набор от критерии за организирането му. Основните характеристики на тези критерии, са както следва:

- дефиниция на компетентността на лицето, подлежащо на сертификация;
- описание на личните качества на знания и умения;
- независими оценявания;
- действителен тест за демонстрация на компетентността.

2.2. Сертификация на продукти

Има известен брой схеми за сертификация на продукти, макар и далеч по-малко, отколкото са за хората. Може би най-добре познатата схемата е Общи Критерии (Common Criteria, известна още като ISO / IEC 15408), но има още няколко други правителствени и търговски схеми, които сертифицират определено ниво на сигурност за даден продукт.

Това са уникален набор от критерии, валидни за всяка IT система, за описване на функционалностите, свързани със сигурността (изисквания за функциониране на сигурността) и постигнатото ниво на сигурност (изисквания за уверение за сигурност), както и набор от седем нива на сигурност, съчетавайки редица изисквания за увереност (EAL – Evaluation Assurance Level – ниво за оценяване на уверението за сигурност).

Общите Критерии често са били популяризирани и насърчавани от правителствата и са приведени в център на вниманието. Подобна формална методология за сертифициране на сигурността осигурява солидна основа, върху която да се изгради увереност за сигурност. Това са набор от инструменти, които трябва да бъдат персонализирани за всяка област. Въпреки това те трябва да бъдат завършени с практическо изпълнение на детайлите за специфични продуктови гами и Борда по Методологията на Общите Критерии (Common Criteria Methodology Board) се събира редовно, за да обсъди възможните интерпретации на критериите, условията за изпълнение и необходимите актуализации.

Общите критерии (Common Criteria – CC) в действителност са мета-стандартен набор от инструменти за определяне на ползването на процедури за сигурност за информационни системи. По поръчка от американската „Orange Book” те не съдържат предварително определени „класове на сигурност“. Тези класове са формулирфани в Общите Критерии на базата на специфични изисквания за системата.

От софтуерна гледна точка CC могат да бъдат разглеждани като набор от библиотеки, помагащи да се пишат смислени програми, като например справки за сигурност, профили на защита и т.н.

Подобно на „Orange Book”, Общите Критерии съдържат два основни типа изисквания към сигурността:

- Функционални – съответстващи на активния аспект на защитаването и представянето на функции, и изпълнени в тях механизми за сигурност;

- Изисквания за доверие – съответстващи на пасивния аспект на защитата на технологията на системата и процеса на нейното разработване, внедряване и експлоатация.

По отношение на изискванията за доверие, в Общите Критерии са въведени седем оценяващи нива на доверие, съдържащи комбинации от рационализирани компоненти.

Първото ниво осигурява анализ на функционалните спецификации, спецификации на интерфейси, документация по изпълнение, но също така и независимо тестване. Първоначалното ниво се прилага в случаите, когато заплахите не се считат за сериозни.

Второто ниво, в допълнение на първото, осигурява допълнително оценяване, подбор на независими тестове, анализ на устойчивостта на функциите за сигурност, искания от разработчика на явни уязвимости.

В **третото ниво** се провежда контрол на околната среда, също така се извършва разработване на конфигурация и управление на съоръженията за оценяване.

На **четвъртото ниво** се добавя следното: пълна спецификация на интерфейсите на проекти на ниско ниво, анализ на подгрупи на реализация, внедряване на неформални модели на политики за сигурност, независим анализ на уязвимости, автоматизация на управлението на конфигурацията. Несъмнено това е най-високото ниво, което е трудно за постигане с традиционните методи на програмиране и допустимите разходи.

На **петото ниво**, в допълнение към предходните, се осигурява използването на формални модели на политики за сигурност, и функционални полу-формални спецификации с демонстрация на съответствието между тях. Необходимо е да се изпълнят анализи на скрити канали от разработчиците и проверяващите.

Шестото ниво на реализация на сертификацията е представено по структуриран начин. Анализът на съответствието трябва да бъде удължен до най-ниските нива на проектиране и програмиране.

Най-високото (седмо) оценъчно ниво предоставя формална проверка на проектите за оценка на обекти. То се прилага в ситуации на много висок риск.

2.3. Сертификация на процеси

Преди години имаше редица стандарти за сертифициране на процес в сферата на информационна сигурност. Страни и браншови асоциации имаха свои собствени идеи за това как да се имплементира информационната сигурност. Много от тези стандарти са все още широко използвани, било то с фокус върху националните изисквания (като например специфични езици (не-английски)) или с фокус върху специфичен пазарен сектор.

Въпреки това все по-често, и особено в организации, които са еднакво активни в повече от една страна, ISO 27001 се превръща в стандартът на избор за управленческа система за сертификация на информационната сигурност на дадена организация. Това е особено удобно в страни, където вече се е използвал неговият предшественик - Британският Стандарт BS7799, или някой от неговите национални вариации. Вече има повече от 70 страни, извършващи сертификация, базирана на 27001 и над 47 сертифицираши органи.

Един от основните въпроси около ISO 27001 е дали той е подходящ за организации с различни размери. Някои критици твърдят, че стандартът е сложен и скъп за изпълнение, както и че не е приложим за по-малките организации – необходима е опростена ISO 27001 версия. Въпреки това, поддръжниците на ISO 27001 предупреждават, че олекотена версия ще размие ценността на сертифицирането. Всичко, което в действителност е необходимо, е конкретно да се насочват малките и средните компании за това как да се прилага ISO 27001 успешно.

Една олекотена версия също така ще добави към объркването при именуването, причинено от прехода от Британския Стандарт (British Standart - BS) към Международния Стандарт (International Organization for Standardization - ISO), и продължаващото разширяване на фамилията стандарти ISO 27xxx.

Важно е да се отбележи, че ISO 27001 не е технически стандарт. Той най-вече има отношение по управлението на риска. Също така не е зрял модел, който да каже на една организация колко добре позициониран във връзка с информационната сигурност. По-скоро е модел за непрекъснато усъвършенстване. Когато компания се стреми за тази сертификация, тя не иска просто уплътнение, което да показва; тя иска нещо, което е ценно в контекст.

Въпреки това една компания, сертифицирана по ISO 27001, може разбира се да използва този сертификат като маркетингов инструмент, например на брошури, фирмени бланки и реклами, въпреки че тя не може да го използва за рекламиране на даден продукт, защото ISO 27001 е схема за сертифициране на система, а не продукт . Какво точно е включено:

- Класификация на информационните качества;
- Оценка и управление на риска;
- Контрол на достъпа;
- Управление на работните процеси;
- Защита срещу нежелан софтуер;
- Мониторинг и управление на инциденти;
- Физически мерки за сигурност;
- Сигурност за персонала.

3. Сертификация в България

3.1. Структура на системите за сертификация

Системите за сертификация са изградени в съответствие с изискванията, съдържащи се в някои ръководства на ISO от постоянния комитет за сертификация. В съответствие с изискванията на тези ръководства, всяка сертификационна система трябва да включва в структурата си:

- Специален орган по сертификация – това е правителствен орган, който създава и ръководи системата, който регистрира дадените сертификати и който осъществява контрол по спазване правилата на сертификационната система. В България този правителствен орган се нарича Изпълнителна агенция „Сертификация и изпитване" към министъра на икономиката.

- Орган по акредитация – това също е правителствен орган, който има правото и задължението да упълномощава съответните организации, да извършва сертификация и сертификационни изпитвания. Нарича се Изпълнителна агенция „Българска служба за акредитация" към министъра на икономиката. Тази агенция има правото да упълномощава съответни лаборатории, където се извършват сертификационните изпитвания.

- Сертификационна организация – това е организацията, която е компетентна и упълномощена да извършва сертифицирането и да издава сертификат. Тези организации имат право да издават лиценз за използване на съответния знак за съответния сертификат. За сега в България няма сертификационни фирми, а само представители. Има само една българска сертификационна фирма, но тя е към Министерството на отбраната и тя може да извършва сертификация само на такива продукти.

- Акредитирани лаборатории – това са лаборатории, които са независими от фирмите – производителки и купувачи и които са упълномощени от БСА да извършват сертификационни изпитвания.

- Органи по надзора – това са подразделения на Изпълнителна агенция „Сертификация и изпитвания", на които е възложена задачата да

контролират до колко правилно се извършва сертификацията, до колко фирмите спазват изискванията за сертификация. Тя има 5 регионални звена, които отговарят за контрола върху сертификационната дейност в съответните области.

3.2. Основни процедури при сертификацията

Основните процедури при сертификацията са разработени от Изпълнителна агенция „Сертификация и изпитвания". Основните процедури са:

- Изпращане на заявка – предложение от фирмата – производителка до сертификационната организация. В тази заявка се прави предложение какво и как да се сертифицира. Тя е придружена с комплект от документи – обща характеристика на предприятието, информация за изградената система за управление на качеството и т.н.

- Експертна оценка на възможностите за извършване на сертификация – прави се от експертна група, формирана от сертификационната организация, на основата на постъпилата заявка – предложение.

- Сертификационно изпитване на продукцията – когато предложението се приеме, сертификационната организация сключва договор с фирмата – производителка, където се посочва в кои акредитирани лаборатории трябва да се изпрати продукция за изпитване на съответствията. Съставят се протоколи за съответствие, които се изпращат в сертификационната организация и така се взема решение.

- Одит на фирмата – производител. Фирмата се посещава от специалисти на сертификационната организация (одитори), които проверяват състоянието на фирмата и съставят отчет за одита, който се изпраща в сертификационната организация. Този отчет също е база за вземане на решение от сертификационната организация.

- Вземане на решение във връзка със сертификацията. Взема се от самата организация на база на протоколите от сертификационните изпитвания и отчетите за одита. Има само два вида решения – положително и отрицателно. При положително решение организацията издава сертификат, а може да издаде и лиценз за използване на сертификационния знак.

- Регистрация на сертификатите – след като е издаден сертификатът, той се регистрира в Изпълнителна агенция „Сертификация и изпитване”. Сертификацията влиза в сила от дата, в която се публикува в съответния бюлетин.

3.3. Контрол по спазване на правилата в сертификационните системи

Контролът по спазването на правилата в сертификационните системи е възложен на подразделенията на Изпълнителна агенция „Сертификация и изпитване”. Тези органи следят до колко правилно се осъществява сертификацията, дали фирмите изпълняват правилата на сертификационните системи, следят за валидността на сертификацията. Фирмите се задължават да пресертифицират своята продукция при изтичане на валидността на съответния сертификат или при появата на нов стандарт. Органите по надзора трябва да следят дали качеството на продукцията на съответната фирма съответства на изискванията на сертификата. Най-важната санкция при установяване на несъответствие е предсрочно отнемане на сертификата.

4. Заключение

Под сертификация (оценка на съответствието) се разбира понятието, определените изисквания отнасящи се към един продукт, един процес, една система, един човек, или едно място да са изпълнени. Сертификацията в крайна сметка е една малка стъпка, а именно едно решение, което след провеждане на одит и изготвяне на доклад, определя дали одитираната организация да получи сертификат или не. Всеобщата езикова практика обаче е да се използва думата „сертификация” за целия процес на оценка на съответствието.

Една сертификация трябва да се провежда от независима трета страна. Под това се разбира, че решението за сертифициране трябва да е безпристрастно и тези, които го взимат не трябва да са участвали в разработването, производството или консултирането и т.н. Сертифицирани могат да бъдат продукти, процеси, системи или хора.

5. Задачи за изпълнение

1) Изпълнете всички стъпки по сертифициране на вашата организация.

2) Направете сертификация на хора за информационна сигурност във вашата организация.

3) Направете сертификация на продукти за информационна сигурност във вашата организация.

4) Направете сертификация на процеси за информационна сигурност във вашата организация.