Нов български университет

Управление на мрежовата сигурност

Системи за откриване на нарушители

Доц. Д-р Емил Стоилов

Департамент по Информатика на НБУ

София, март 2011

Съдържание

1 Управление на мрежовата сигурност 3
1.1 Въведение 3
1.2 Политики за сигурност 3
1.2.1 Осигуряване на подкрепа от ръководството 5
1.2.2 Определяне на информационните активи 6
1.2.3 Проект на политическа декларация 7
1.2.4 Оценка на риска 10
1.2.4.1 Присвояване на стойност на активите 12
1.2.4.2 Присвояване на стойност на рисковете 12
1.2.4.3 Мерки за противодействие 13
1.2.4.4 Количествен анализ на риска 14
1.2.4.5 Качествен анализ на риска 18
1.2.4.6 Комбиниране на количествения и качествения анализ на риска 19
1.2.5 Избор на мерки за противодействие 19
1.2.5.1 Анализ на разходите и ползите 20
1.2.5.2 Различни фактори влияещи върху избора на мерки за противодействие 22
1.2.5.3 Административни мерки за противодействие 27
1.2.5.4 Физически мерки за противодействие 29
1.2.5.5 Технически мерки за противодействие 30
1.2.6 Създаване на документация за стандарти и процедури по сигурността 30
1.2.7 Създаване на ръководства за конфигуриране 30
1.2.8 Примери за стандарти по сигурността 31
1.2.8.1 Стандарти за паролите 31
1.2.8.2 Стандарти за маршрутизаторите 31
2 Системи за откриване на нарушители 32
2.1 Общ преглед 32
2.2 Видове IDS 35
2.2.1 Съдържателно претърсващи IDS (Signature-Based IDS) 35
2.2.2 Статистически IDS (Statistical-Based IDS) 36
2.2.3 IDS за хост и IDS за мрежа 37
2.2.3.1 IDS за хост (Host-Based IDS) 37
2.2.3.2 IDS за мрежа (Network-Based IDS) 38
2.3 Настройки на IDS 41
2.4 Разполагане на IDS в мрежата 43
2.5 Реактивни IDS 44
2.6 Интегриране на защитната стена с IDS устройство 45
2.7 Други видови IDS 46
3 Литература 50

1. Управление на мрежовата сигурност

1.1 Въведение

От самото начало трябва да стане ясно, че използваната технология сама по себе си не може да направи вашата мрежа сигурна. Причината е, че в основата на всички технологии за сигурност лежи човешкият фактор. Винаги ще се намери някой, който неправилно ще конфигурира защитните стени, ще издаде на приятелите си паролите, ще направи програмна грешка, която ще срине сървъра при въвеждане на неочаквана входна променлива. Ето защо ние не можем да разчитаме технологията да защитава нашата мрежа. Хората, които са създали тази технология не са съвършени. Със сигурност не трябва да очакваме също технологията да ни предпази от компютърни престъпления. Не бива да се заблуждаваме, че точно ние сме поколението, което е намерило начин да се имунизира срещу престъпленията чрез използване на съвременна технология.

Когато разсъждаваме върху мрежовата сигурност, трябва да мислим като за система, не като за някакъв вид технология. Целта на тази статия е да ви убеди, че вашата информация се защитава с използването на определени политики за сигурност, а не с технологията, която сте решили да използвате.

Повечето хора ясно разбират необходимостта от защита за тяхната мрежа. Почти във всички анкети за допитване до мрежови администратори, директори и мениджъри, на едно от първите три места те поставят проблема за защита на тяхната мрежа от хакери. За съжаление поставянето на този проблем като приоритет неминуемо води до избор на технология, която да управлява сигурността.

Когато технологията е водеща за сигурността, IT персоналът обикновено се концентрира върху защитните стени (firewalls) или върху частните виртуални мрежи (Virtual Private Networks – VPN). Макар че включването на защитната стена в модела за сигурност е явно добра идея, това не е правилният подход към създаване на мрежова сигурност. Концентрирането върху защитната стена води до създаването на модел за сигурност, който е изграден върху това, което може да предложи конкретното устройство, а не върху това от което мрежата има нужда. Преди да говорим за хардуер и софтуер, на първо място трябва да бъде осмислена и създадена конкретна политика за сигурността на мрежата. Политиката за сигурност на мрежата представлява декларации на високо ниво за възприетите принципи и описва нуждите на конкретната мрежа. След като вече знаем какво трябва да постигнем, чак тогава можем да започнем обсъждането на модела за сигурността. Моделът за сигурността е изграден от хардуер, софтуер, както и насоки за конфигуриране, които ще бъдат използвани за прилагането на избраната вече политика.

1.2 Политики за сигурност

Правилно създадената политика за сигурност има много специфична структура. Тя представлява документ от високо ниво, който описва философията, бизнес средата и целите на организацията. За изпълнението на тези цели трябва да бъдат предприети конкретни стъпки. Тук се вижда ролята на стандартите и процедурите по сигурността. Политическа декларация от високо ниво е например следното изискване: „Всички финансови транзакции между бизнес партньорите да остават поверителни и да пристигат с гарантирана непокътнатост”.

Стандартите и процедурите могат по-нататък допълнително да уточняват например, че: „Поверителният характер на данните в мрежите използващи обществен Интернет ще бъде осигурен по един от двата начина:

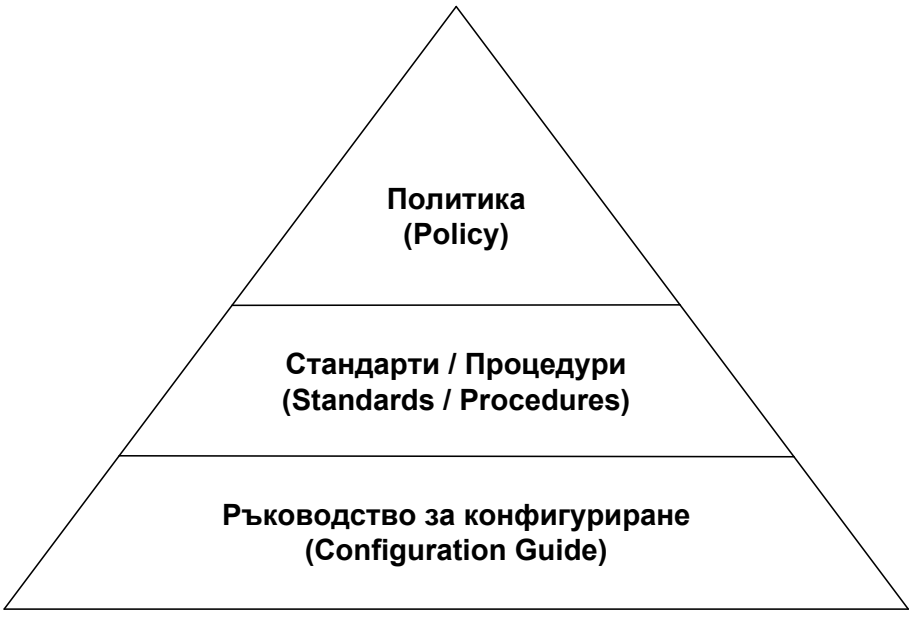
1) Един VPN IPSec канал с 256-битов AES. Установяването на самоличността да се осъществява с RSA подписи чрез защитен механизъм, като подписите бъдат обявявани за действителни от външен сертифициран орган.

2) MPLS базирани частни виртуални мрежи между бизнес партньори, които имат един и същи доставчик на услуги. За гарантиране на целостта на транзакциите се използва null-encryption и алгоритъм за хеширане MD5."

Декларации от този тип дават възможност за използване на различни начини за осигуряване на поверителността и целостта на данните между вашият сървър и отдалечени бизнес партньори.

Само стандартите и процедурите не са достатъчни за реализиране на конкретно решение. Необходими са и ръководства за конфигуриране. Както подсказва името, ръководството за конфигуриране описва стъпка по стъпка кои възможности са разрешени, какви стойности трябва да бъдат използвани и т.н. за да се реализира политиката за сигурност.

Комбинирайки политическите декларации от високо ниво, стандартите и процедурите, както и ръководствата за конфигуриране, структурата на модела на политиката за сигурност може да бъде представена като диаграма подобна на тази от Фиг.1



Фиг. 1 Модел на политиката за сигурност

Процесът на създаване на политиката за сигурност може да бъде разделен на девет отделни стъпки, всяка от която допълнително може да бъде раздробена, ако е необходимо. Тези девет стъпки са представени по-долу.

1. Осигуряване на подкрепа от ръководството
2. Определяне на информационните активи
3. Проект за политическа декларация
4. Оценка на риска
5. Избор на мерки за противодействие
6. Създаване на стандарти за сигурност
7. Създаване на ръководства за конфигуриране
8. Прилагане на политиката за сигурност
9. Преразглеждане и изменение на политиката за сигурност

Следва описание на тези стъпки в подробности.

1.2.1 Осигуряване на подкрепа от ръководството

Понякога е трудно да се обясни на ръководството на фирмата защо трябва да се положат много усилия, да се загубят време и пари, за да бъде изградена политика за сигурност. Без това обаче да бъде направено, работата по останалите стъпки в процеса на изграждане на политиката за сигурност е до голяма степен безсмислена. Тази стъпка е неразделна част от успешното реализиране на мрежовата сигурност и е абсолютно необходимо тя да бъде направена до пълното установяване на параметрите на сигурността в мрежата.

Съществуват практически и правни съображения ръководството на фирмата да участва в изграждането „отгоре-надолу" на политиката за сигурност от самото начало на процеса на проектиране. Запомнете: вие не можете просто да доставите няколко мрежови технологии и да очаквате с тях да се постигне необходимата сигурност. Най-голямо подобрение на сигурността се получава, когато се извърши и промяна в поведението на индивидите, участващи в процеса. Такава промяна обаче не може да се осъществи без намесата на органа за управление.

Създаването на политика за сигурност от „долу нагоре", когато няколко изтъкнати IT специалисти обсъждат пътищата за подобряване на сигурността на мрежата, е неефективна като практика. Приоритетите на IT персонала по всяка вероятност ще се различават съществено от приоритетите на ръководството. Когато тези две гледни точки влязат в конфликт, познайте кой печели най-често? Практическата причина за получаване на подкрепата на ръководството е съвсем проста – без тази подкрепа политиката за сигурност бързо ще се маргинализира и всички ще се разочароват от нея.

Правната обосновка е много по-сложна. В повечето страни ръководството на една организация носи финансова отговорност пред собствениците на фирмата. В публично търгуваните компании това са акционерите. При разглеждане на въпроса за отговорността на висшите длъжностни лица, когато сигурността е нарушена, има няколко понятия с които трябва да сме запознати. Те са *due diligence (надлежна проверка)*, *due care (дължима грижа)*, и *prudent man rule (принцип на предпазливия човек).*

Много често естественият инстинкт ни кара да мислим, че всички компютърни престъпления са по вина на хакери. В края на краищата, хакерите са тези, които нарушават закона. От юридическа гледна точка обаче, това е само една част от истината. Ако дружеството се търгува публично и ръководството не е взело мерки за защита на важни фирмени данни, с което е улеснило хакерите, то също носи лична юридическа

отговорност за загубите. При определяне на вината или невинността на член от ръководството се взимат под внимание споменатите по-горе *due diligence*, *due care*, и *prudent man rule* като те се преценяват внимателно спрямо фактите по делото.

Due diligence се отнася за дейности, които гарантират непрекъснатата поддръжка на защитата на мрежата. Това означава, че има изградена организация за защита на мрежата в нормални условия и ролите на IT инженерите и персонала по сигурността са точно дефинирани и определени. *Due diligence* може да се докаже със съществуването на политика за сигурността и нейното правилно приложение.

Due care се отнася до стъпките, които дадена компания е предприела, за да покаже, че е поела отговорност за действията, които се извършват в нейните граници, с нейните ресурси, както и с нейните служители. Разбира се, част от тези ресурси са мрежови компоненти. Голяма част от стойността на една фирма е информацията в базата данни, която от своя страна се намира в мрежата. Ако тази информация не е надлежно защитена, значи не се полага *дължимата грижа (due care).*

И накрая ръководството трябва да спазва *принципа на предпазливия човек (prudent man rule)* когато се определя дали се извършват надлежните проверки и полагат дължимите грижи правилно. Този принцип изисква ръководството при изпълнение на своите задължения да действа „благоразумно", както действат предпазливите хора при подобни обстоятелства.

Могат ли ръководителите да одобрят инсталирането на защитна стена и да твърдят, че с това изпълняват законовите задължения на дружеството? Зависи. Ако обектите, които те се опитват да защитят (т.е. данни, хардуер, персонал, дори и собствените си репутации) не са критични и мрежата е уязвима и застрашена от IP пакетни атаки, тогава може да се твърди, че принципът *prudent man rule* е спазен. От друга страна, ако мрежата включва критични елементи и е привлякла вниманието на добре финансирани криминални престъпници или дори чужди правителства, които биха могли да инициират различни широко мащабни атаки, то би било трудно да се твърди, че принципът *prudent man rule* е приложен правилно. В този случай защитната стена не би могла сама по себе си да осигури необходимото ниво на защита на данните.

Въпросът тогава стои по следния начин: как може ръководителят да определи дали принципът е приложен правилно? За да се получи отговор на този въпрос е необходимо да се направи анализ на риска.

1.2.2 Определяне на информационните активи

Активът е нещо ценно, което компанията притежава. Това може да бъде интелектуална собственост, търговски тайни, авторски права, бази данни, работни станции, сървъри, маршрутизатори, принтери и т.н. За да изградим политиката за сигурност ние трябва да сме наясно с приоритетите в нашата мрежа. За получаването на тази информация е необходимо да се направи подробна инвентаризация на всички хардуерни и софтуерни активи, както и да се проведат разговори на всички нива на управленската структура. Изясняването на въпроса кои ресурси са приоритетни за компанията е от изключителна важност.

В някои случаи нямаме голяма гъвкавост при избора на това, върху което трябва да акцентира политиката за сигурност. Например изискванията за информационна сигурност често са регламентирани или наложени от промишлеността или търговски групировки. Затова преди да създадем проект на политиката за сигурност трябва да се убедим, че всички регламентирани нормативни изисквания са взети предвид.

1.2.3 Проект на политическа декларация

Преди да започнем анализа на риска и създаването на политиката за сигурност е необходимо да уточним някои понятия. По-късно ще посочим, че политиката трябва да бъде написана на език, който да бъде лесно разбираем от крайния потребител. По време на обсъждането на политиката обаче ще се води спор между IT професионалисти по сигурността, така че употребяваните термини трябва точно да отговарят на техните дефиниции.

При създаването на политиката за сигурност първо трябва да си поставим въпроса какво целим да постигнем. Това би трябвало да изглежда просто – по-сигурна мрежа разбира се! Но какво дефинира сигурна мрежа? Професионалистите по сигурността обичат да описват сигурната мрежа като такава, която поддържа три основни цели:

1) **Поверителност (Confidentiality)**. Казано по-просто, това е очакването, че личните данни ще останат лични. Отнася за всякакъв тип данни. Например това може да означава, че говорейки за бази данни, достъп до конкретни елементи на базата ще имат само тези потребители, които имат разрешения за това. Потребители, които нямат разрешение, но успеят да прихванат пакети от мрежата не трябва да имат възможност да дешифрират информацията в тях. При друг случай това може да означава, че личните файлове на потребителите намиращи се върху файлов сървър или настолен компютър не могат да се четат от тези, които нямат необходимите разрешения. При трети случай се вижда, че фирмата не се вълнува особено, когато се прихващат потребителски данни, като например такива свързани с електронната търговия, номерата на кредитните карти и други. Във всеки от горните случаи има очакване за поверителност, но начинът по който тази поверителност се постига във всеки случай е различен. Една политика за сигурност трябва да разгледа въпроса при какви обстоятелства каква поверителност се очаква от потребителите. Един потребител, който използва IPSec за създаване на VPN между две точки, няма да направи нищо за защита на данните, които вече се съхраняват върху файлов сървър. Прилагането на различни нива за достъп до файл няма да помогне с нищо, ако упълномощеното лице изпраща информация по мрежата, където тази информация може да бъде прочетена от всеки снабден с програма за прихващане и анализиране на пакети.

2) **Интегритет (Integrity)**. Интегритет е очакването, че данните които чете потребителят са в техния оригинален, авторизиран и непроменен вид. Това не означава, че данните не могат да бъдат променяни. Промяна на данните може да се извършва само от упълномощените (авторизирани) за това лица. Например данните изпратени по мрежата като електронна поща могат да бъдат прихванати, променени, и след това изпратени на получателя. В този случай получателят трябва да знае, че не всичко е както изглежда. Друг пример са файлове върху файлсървър, съдържащи информация за дългове. Криминален престъпник може да бъде заинтересован повече да промени данните, отколкото да ги прочете. Целта му

е да намали дълга. Както при поверителността, горните примери са свързани с очакването на потребителя за интегритета на данните. Този интегритет може да бъде постигнат по различени начини.

3) **Наличност (Availability)**. Наличността е гаранция, че данните са на разположение, когато потребителите очакват това. Един от най-простите начини да се наруши нормалното функциониране на мрежата е да се направи тя недостъпна. Докато компрометирането на поверителността и интегритета обикновено изисква определени познания и умения от страна на атакуващия мрежата, то отказът за достъп до мрежови ресурси (известен като „отказ на услуга" DoS) може да бъде постигнат сравнително лесно, с използването на не особено елегантни методи. Наличността може да бъде прекъсната по много начини, и всеки един от тези начини се нуждае от различно противодействие за намаляване на риска. Блокиране на потребителските имена или въвеждане на вирус от типа „троянски кон" може да попречи на достъпа на потребителите до техните собствени компютри. Промяна на настройките на комутаторите и маршрутизаторите или просто генериране в мрежата на повече трафик водещ до нейното задръстване, ще попречи на комуникацията с отдалечените сървъри. И накрая, като атакуваме крайната точка на комуникационния процес и блокираме отдалечения сървър, също ще прекъснем достъпа на потребителите до техните данни. Влияние върху наличността може да окаже и нещо толкова просто, като изключване на захранването на сървъра. Ясно е, че много елементи трябва да се вземат предвид за да осигурим наличност на мрежовите ресурси за потребителите. Всеки един от тези елементи носи различен риск и трябва да бъде включен в политиката за сигурност.

Когато започнем да разглеждаме основните заплахи за мрежата ще се убедим, че те в голяма степен застрашават тези три главни цели на политиката за сигурността.

Политиката за сигурност може да приема различни форми; представената по долу представлява само едно предложение. Съществуват обаче няколко характеристики, които всяка форма трябва да притежава.

На първо място тя трябва да е лесна за четене и лесно да се ориентираме в нея. Трябва да бъде написана ясно и точно, без препратки към други документи, без съкращения, но и без излишни обяснения. Ако тя е така написана, няма да има случай някой да оспори политиката за сигурност в защита на собствените си действия. Това може да се случи само когато има двусмислие в текста или неясноти в използваните термини и определените срокове.

Политиката за сигурност обикновено има следните раздели:

- **Въведение (Резюме)**. Въведението (или Резюмето) описва документа и неговото предназначение – предоставяне на информация относно позицията на организацията по отношение на информационната сигурност.

- **Контекст**. Тук следва да се посочи всяко влияние върху създаването на политиката за сигурност. Например: „Като публично търгувана корпорация, ние имаме отговорността да …". Освен това всички закони и подзаконови актове, които засягат политиката за сигурността трябва да бъдат въведени в този раздел.

- **Декларация за политика**. Това е основната част на документа. Не забравяйте, че това е изявление от високо ниво относно политиката, затова рядко се случва то да бъде по-дълго от няколко страници. Тук трябва да се акцентира върху такива думи като „поверителност", „интегритет", „наличност", както и да се изясни организацията на информационните активи. Например, „Нашият бизнес разчита на непрекъснатост на Интернет и на вътрешната електронна поща. Интегритета на всички данни произхождащи от нашата компания не трябва да се поставя под съмнение. Освен това, нашите клиенти могат да разчитат, че поверителността на техните данни ще остане ненарушена".

- **Дефиниции**. Всичко това, което може да бъде оспорено по някакъв начин, трябва да бъде дефинирано тук. Основната цел на този раздел е да се постигне четливост на политическите изявления и да позволи на потребителите по-лесно да намират информация изясняваща политическите декларации.

- **Органи / Отговорности**. Политиката за сигурност трябва точно да посочи кой от ръководството я поддържа. Този раздел трябва да съдържа информация за това кой практически осъществява тази политика и кой носи отговорност за нейното приложение. И накрая, какви санкции са предвидени за неспазване на политиката за сигурност и кой ги прилага. Много важно е да бъдат включени арбитражни процедури при налагането на такива санкции.

- **Промени в политиката за сигурност**. Политиката за сигурност търпи промени с течение на времето. Трябва да има преразглеждане на целите на политиката поне веднъж годишно. Преразглеждане трябва да се прави и след всеки компютърен инцидент. Потребителите на мрежата също могат да поискат промяна на политиката за сигурността с цел използване на нови услуги, необходими за тяхната работа. Следователно промените трябва да засягат и процедурите с които потребителите могат да изискват промени в политиката за сигурност.

- **Достъпност на информацията**. Всеки служител трябва да има достъп до политиката за сигурност на организацията. Този достъп трябва да бъде осигурен от тези, които създават политиката. Те отговарят и за това потребителите да са запознати с всички промени и актуализации на самата политика.

Политиката за сигурност може да бъде придружена и от други, допълнителни документи засягащи информационната сигурност. Най често срещаните такива документи включват политика за одобрено използване (Accessable Use Policy), политика за отговорност при инциденти (Incident Response Policy) и план за възстановяване и продължаване на работата (Disaster Recovery/Business Continuity Plan). Всеки един от тези документи се създава по начин подобен на създаването на политиката за сигурност. Разликата е, че политиката за сигурност се счита за основна схема, а всеки от допълнителните документи подкрепя общите цели залегнали в политиката за сигурност. В известен смисъл всеки от тях съдържа отделни стандарти и процедури, но в крайна сметка описва как целите на политиката за сигурност се изпълняват.

1.2.4 Оценка на риска

Оценката на риска е неразделна част от процеса на създаване на информационна сигурност. Ние не можем да създадем политика за сигурност, която да отразява нашите изисквания и да намалява риска до приемливо ниво, докато не получим ясна картина какви са рисковете, които застрашават нашите активи. В този раздел разглеждаме накратко изкуството и науката за определяне на риска. Когато се извърши правилно, оценката на риска ни дава верен отговор (в пари и усилия) за резултатите които ще бъдат постигнати при прилагането на политиката за сигурност. Изграждането на политиката за сигурност е многоетапен процес. Първо се определя какво трябва да се защити, след това се определя от кого трябва да защитаваме нашите данни и вероятните рискове пред които ще се изправим.

Предварителната работа, която трябва да се извърши е известна като анализ на риска. Анализът на риска се категоризира в две основни групи:

1) *Количествен анализ*, при който се опитваме да припишем стойност на всеки актив и да сравним тази стойност с цената на свързаната с актива заплаха и
2) *Качествен анализ,* който изисква от хората по-дълбоки познания за компанията.

И двата подхода имат своите добри и лоши страни. В крайна сметка се извършва компромис между тях, и този компромис се възприема за основа на политиката за сигурност.

За да разсъждаваме върху риска е необходимо няколко понятия да бъдат изяснени. Първото от тях е самото понятие „риск". Рискът се дефинира като вероятност от *заплаха (threat)*, възникнала вследствие на *уязвимост (vulnerability)* на мрежата.

Уязвимостта е слабост на мрежата, която слабост може да бъде използвана от хакер. При обсъждането на всички аспекти на сигурността на мрежата ще се убедим, че броя на уязвимите места е просто зашеметяващ [1], [2]. Като уязвимости можем да изброим например отключените врати на сървърните помещения, ненужни услуги, които се изпълняват върху сървърите, архивирането на данни, когато не се извършва редовно и т.н. Лесните за отгатване пароли представляват уязвимост, но принуждаването на потребителите да използват трудни за отгатване пароли (и съответно трудни за запомняне) създава друга уязвимост.

Заплаха е всяка опасност за активите на организацията. Това може да бъде лице (нищо не подозиращ служител или злонамерен хакер), природно бедствие или даже чужда нация. Всяка една от тези заплахи може да води до нарушаване на политиката за сигурност на компанията. Докато хакерът например иска да разруши поверителността на информацията, нищо не подозиращият служител, опитвайки се да увеличи своята производителност, може да наруши интегритета на данните. Земетресение в Сан Франциско, от друга страна, би могло сериозно да засегне наличността на конкретни данни за потребители от цял свят.

Когато заплахата има шанс да се възползва от уязвимостта, тогава съществува риск, на който трябва да се обърне внимание. Уязвимостта от незаключената врата на сървърното помещение, в комбинация със заплахата от злонамерен служител, създава риск, които може да се отрази на поверителността, интегритета и наличността на данните едновременно. Използването на само едно място за съхранение на архивираните данни,

в комбинация с катастрофален пожар, създава риск, който сериозно ще се отрази на наличните данни.

Обобщавайки, фигуративно можем за запишем:

Threat + Vulnerability = Risk

Когато една компания търпи загуби вследствие на заплаха, това е известно като *реализация на риска* (Употребява се също и терминът *„изобличаване”* (*exposure*)). В момента когато злонамерен служител (заплаха), премине през незаключената врата на залата със сървъри (уязвимост), и започне да изключва сървърите, компанията, оставила входа незаключен, претърпява реализация на риска. Накратко, реализацията на риска е това, което повечето компании се опитват да предотвратят след като са осъзнали съществуването на комбинацията от заплаха и уязвимост.

За намаляването на възможността за реализация на риска е необходимо да бъдат предприети *мерки за противодействие (countermeasures)*. Като противодействие на заплахата от незаключена врата може да се приложи един от най-ефективните методи измислени засега – вратата просто да се заключи. Забележете, че в този случай противодействието е успешно, защото премахва уязвимостта, а следователно и намалява възможността за реализация на риска. Тази ответна мярка, обаче, не оказва влияние върху заплахата. Уязвимостите са слабости, които могат да бъдат предотвратени. Заплахите, от друга страна са потенциални опасности от всякакъв вид. Заплахите никога не могат да бъдат напълно премахнати, с тях трябва винаги да се съобразяваме..

От дискусията дотук можем да заключим, че уязвимостите са фактор, върху който собствениците на мрежата имат контрол. Заплахите са тези външни елементи, върху които контрол нямаме. Здравият разум ни подсказва, че трябва да откриваме уязвимостите и да предприемаме мерки срещу тях. Заплахите трябва да бъдат анализирани и тяхното въздействие да бъде оценявано.

Това, че съществува риск, не означава, че той трябва да бъде подробно разглеждан в политиката за сигурност. Строго погледнато, съществува и риск от нападение на извънземни от друга слънчева система, които да се възползват от уязвимостта на нашата мрежа, а именно, че около нея няма изградена енергийна защита срещу техните оръжия. Изграждането на такава защита е изключително скъпо и трудно бихме могли да обясним на събранието на акционерите нейната целесъобразност. Това разбира се е в сферата на фантастиката, но други примери могат да не бъдат толкова очевидни. Събитията от 11 септември 2001 година в САЩ са пример в това отношение. Трябва да има начин да се позволи на специалистите по сигурността и администраторите на мрежата да определят от кои рискове си струва да се защитаваме и от кои не. Този процес е известен като *анализ на риска (risk analysis).*

Анализът на риска ни позволява да подредим рисковете в една система и на базата на възможните щети при реализация на тези рискове, да оправдаем направените разходи за сигурността. След като рисковете са идентифицирани и са определени евентуалните загуби от тяхната реализация, чак тогава можем да започнем процеса на *управление на риска (risk management).* Управлението на риска представлява процес на намаляване на риска до приемливо ниво, прехвърляне на риска на други субекти като например застрахователни дружества, отхвърляне на риска или просто неговото приемане.

Както вече беше споменато, при анализа на риска имаме количествен и качествен подход. Всеки един от тях има своите предимства и недостатъци. За целите на политиката за сигурност количественият и качественият подход трябва да бъдат разглеждани като взаимно допълващи се. За да извършим ефективна оценка на риска е необходимо да приложим и двата подхода.

На високо ниво процесът на анализ на риска включва три стъпки:

1) Присвояване на стойност на активите

2) Присвояване на стойност на рисковете

3) Избор на мерки за противодействие, съответстващи на стойността на активите и на разходите при реализация на рисковете.

1.2.4.1 Присвояване на стойност на активите

При задаване на стойностите срещаме различни елементи. Някои от тях са съвсем очевидни, като например разходи за поддръжка и замяна на актива. Други са малко по-сложни, например колко струва този актив на нашата фирма, и колко би струвал той за нас, ако го притежаваше конкурентна фирма. Всички тези елементи трябва да бъдат разгледани, когато определяме стойността на даден актив.

Информацията за оценка на актива може да идва от няколко източника. Финансовият отдел е един от тях. От там можем да научим стойностите на придобиване, поддръжка и разходите за подмяна на хардуера и софтуера. IT персоналът също може да бъде много полезен когато определяме разходите при прекъсване на работата на мрежата и щетите, които всяка една заплаха може да причини в системата.

Понякога не е лесно много важна ценност за организацията да се определи само с финансови параметри. Каква е например стойността на репутацията на компанията? Някои компании губят над милиард долара от пазарна декапитализация вследствие на излезли наяве скандали в ръководството. Много фирми дори не докладват за компютърни престъпления, защото смятат, че общественото доверие в компанията ще се влоши, ако тази информация стане публична. Ако вашата компания предлага продажби по Интернет, какви ще бъдат разходите на дружеството, ако се установи, че във вашия уеб сайт са проникнали хакери? Разбира се, вие съхранявате базата с данни на друг сървър и информацията за клиентите не е компрометирана, но как тях ще ги убедите в това и как ще възстановите тяхното доверие? В този случай загубите за вашата компания ще бъдат осезаеми, но тяхното остойностяване предварително ще бъде доста трудно.

1.2.4.2 Присвояване на стойност на рисковете

В процеса на оценка на риска, когато присвояваме стойност на конкретен риск, официално се използва понятието *очакване за единична загуба (single loss expectancy - SLE)*. На базата на сравнения определяте колко ще загуби вашият актив при реализация на всеки риск. Например, колко ще ви струва, ако някой изхвърли мрежов сървър през прозореца? Колко ще ви струва да възстановите данните от този сървър? Каква би била стойността на загубата от производителност? Тъй като всеки един от тези рискове е с

различна степен на свързаните разходи, за всеки актив трябва да бъдат дефинирани множество рискове. Припомняйки си дефиницията за риск, ще представим няколко примера за да се изясни понятието присвояване на стойност на риск.

Ако има заплаха хакер да компрометира нашия уеб сървър като използва уязвимост на сървърния софтуер HTTP, най-малкото което трябва да направим е да възстановим сървъра от оригиналния носител или от архивирано копие. Това може да отнеме няколко часа, през което време сървърът не е на разположение. Какви ще бъдат разходите свързани с възстановяването от този риск, ако това нещо се случи, т.е. ако настъпи реализация на риска?

Друг пример може да бъде заплаха от заразяване с вирус на клиентски системи, поради използване на остаряла антивирусна програма. В система от 25 потребителя, какви ще бъдат разходите свързани с отстраняването на нанесените щети? Най-малкото, което трябва да се направи е да се инсталира нова антивирусна програма и да се обучат потребителите да работят с нея. Разходите при реализация на този риск са свързани със загубата на време за извършване на тази дейност. Има и загубата на производителност за част от потребителите през този период. Това е твърде оптимистична оценка, тъй като се приема, че няма допълнителни щети нанесени на операционните системи.

Когато определяме стойността на един риск, не е достатъчно да определим очакването за единична загуба, за да вземем нашите финансови или ресурсни решения. Трябва да знаем и колко често рискът ще се реализира или най-малкото вероятността за това.

Да разгледаме случай с вирус в електронната поща. Да приемем, че през последните пет години имаме проникване на вирус чрез прикачени файлове средно два пъти годишно. Това е риск на който е подложена компанията и срещу него трябва да бъдат взети съответни мерки, но той се реализира сравнително рядко. Ако вашата компания обаче е обект на автоматични мрежови атаки, то те могат да бъдат подновявани по няколко пъти на ден. Годишната реализация на риска от заразяване с вирус в този случай е висока.

1.2.4.3 Мерки за противодействие

Сравнявайки средната годишна цена на всеки риск със стойността на дадения актив, можем да дефинираме стойност, която да бъде полезна на компанията за да определи колко си струва да се изхарчи всяка година за защита на активите от различни рискове. Хипотетично казано, ако компанията установи, че ликвидирането на вирусна атака на нейната мрежа струва 20 000 € и статистиката показва че имаме две такива нападения годишно, то този риск в крайна сметка ще струва на компанията 40 000 € годишно. Това би трябвало да бъде и максималният бюджет за прилагане на мерки за противодействие срещу такъв риск. Ако инженерите и администраторите в IT отдела намерят начин да ликвидират риска и предприетите от тях мерки струват по-малко от 40 000 €, то тези мерки би трябвало да се приложат. Ако по някаква причина се установи, че рискът не може да бъде ликвидиран за по-малко от 60 000 € годишно, то компанията трябва да направи избор. От чисто финансова гледна точка предприемането на такива скъпи мерки няма смисъл, тъй като компанията ще спести 20 000 € всяка година, като не върши нищо друго, освен да ликвидира последиците от вирусните атаки. При избора на компанията влияят и други фактори, например нарастването на броя на годишните атаки може да наклони решението в друга посока. В някои случаи разходите за намаляване на риска до приемливо ниво са по-големи от стойността на актива, който се опитваме да защитим. И

макар целта на анализа на риска е да намерим интелигентен начин за неговото намаляване като предприемем мерки за противодействие, то в някои случаи най-интелигентното нещо което можем да направим е да прехвърлим отговорността върху друг или просто да приемем този риск.

Когато разходите за противодействие са твърде високи за да бъдат поети от компанията, тя може да реши да възложи риска на друга страна. Това се нарича „получаване на застраховка”. Същата стратегия, както при застраховането на домашното имущество, може да се приложи и по отношение на мрежовите ресурси. Ако разходите за възстановяване на мрежата при катастрофално събитие са твърде големи, рискът може да се прехвърли на застрахователна компания, която да възстанови щетите след възникване на събитието.

При решение за приемане на риска, компанията просто ще поеме разходите когато събитието се случи. Приемането на риска е подходящо за случаите, когато цената за намаляване на риска е твърде висока. Например когато събитието се случва изключително рядко, или защитата е толкова скъпа, че съответните мерки са нереалистични. При този подход има и елемент на шанс. Понякога приемаме риска просто защото това е най-лесното решение и се надяваме, че когато събитието се случи, ние няма да сме вече в този бизнес.

Задълбоченият анализ на риска преследва две цели:

1) Позволява на служителите по сигурността и финансистите да вземат правилни и обосновани решения по въпроси засягащи мрежовата сигурност.

2) Може да служи като доказателство за предприети разумни действия от страна на ръководството за защита на ресурсите на компанията.

Преди да продължим, да обобщим изложеното дотук. За да определим колко да изхарчим за информационна сигурност трябва:

1) да бъде оценена стойността на информационните активи,

2) да бъдат изброени рисковете, с които се сблъскват тези активи и цената която трябва да се плати, когато тези рискове се реализират,

3) да се изберат мерки за противодействие, които мерки се определят въз основа на тяхната ефективност и разходите по приложението им, сравнени с цената на риска.

1.2.4.4 Количествен анализ на риска (Quantitative Risk Analysis)

След като обсъдихме целите на анализа на риска, по долу ще се спрем на някои особености.

Първата стъпка при анализа на риска е събирането на данни. В крайна сметка нашите решения се основават на първоначално събраните данни. Процесът на събиране на данни трябва да се извърши методично. Като начало се създава списък с всички активи на компанията. На всеки актив се присвоява парична стойност. Не забравяйте, че това не е просто стойността на придобиване. Тук се включват разходите за замяна на актива,

стойността на актива за конкурентите, влиянието, което активът оказва върху рентабилността на предприятието и т.н.

Например първоначалната информация може да бъде от рода „сървър за база данни 60 000 €". В интерес на потребителя е тази стойност да бъде разделена на своите съставни части, колкото е възможно по-подробно. Самият сървър може да бъде оценен на 15 000 €. Базата данни от друга страна може да има стойност за потребителя 45 000 €. Причината за това разграничаване е, че всеки елемент може да има различна уязвимост и да е подложен на различни заплахи. Въпреки че при пожар или експлозия ще бъдат унищожени и двата елемента, за управление на риска могат да се приемат различни мерки за противодействие за всеки актив. Базата данни може да бъде архивирана всяка вечер и резервните копия да се съхраняват в отдалечено от сървърната зала място. За компания, която е стандартизирала платформата на своите сървъри, може да се поддържа отделен сървър, който служи за архивиране, но едновременно с това да е „горещ резерв" и в случай на нужда да замени някой от дефектиралите сървъри.

Разделянето на съставни части при дефинирането на активите позволява да се направи по-точен избор. Раздробяването не трябва да отива и до крайност, тъй като в този случай няма да бъдем в състояние да анализираме и осмислим големия брой активи.

Рисковете, на които всеки актив е подложен, трябва да бъдат изброени. Със всеки един от тези рискове са свързани и потенциални загуби, които ще понесем, ако даденият риск се реализира. Определянето на тези загуби е доста трудно. Ще изясним това с примери.

Фактът, че неоторизирано лице (например хакер) е получило достъп до сървъра означава, че най-малкото което трябва да направим е да възстановим системата от оригиналния носител или от резервно архивирано копие. Нека приемем, че това ни струва 2000 € труд. Ще имаме и загуба в производителността на тези, които разчитат на този сървър; нека тази загуба да бъде 8 000 € . Следователно в електронната таблица за анализ на риска трябва да има ред, съдържащ следната информация:

Сървър Хакер 10 000 €

Тази стойност от 10 000 € е известна като *очакване за единична загуба (single loss expectancy – SLE)* от риск „Хакер". Друг риск може да бъде повреда на дънната платка вследствие на токов удар. В този случай данните и операционната система могат да са непокътнати, но сървърът няма да работи докато не се смени и тества дънната платка. За целите на дискусията, нека приемем, че цената на резервните части и труда по подмяната създава потенциална загуба от този риск възлизаща на 2 000 € и загуба от производителност на още 14 000 €. Следователно в таблицата за анализ на риска за този актив трябва да има нов ред:

Сървър Критичен хардуерен срив 16 000 €

Като последен пример да включим риска от природно бедствие, торнадо. В този случай торнадото ще унищожи целия сървър. Хардуерът ще бъде неизползваем и трябва да се смени. Трябва да се възстанови от архив и цялата информация на сървъра. Ще имаме нов ред в таблицата:

Сървър Природно бедствие – торнадо 45 000 €

Има и друг начин за определяне на SLE. За да го изясним въвеждаме понятието *фактор на очаквано поражение (Exposure Factor – EF)*. Това е субективна, потенциална загуба на определен актив, която загуба е изразена в проценти и е следствие на реализирането на специфична заплаха. Факторът на очакваното поражение е субективна стойност, която лицето оценяващо риска трябва да дефинира. Когато например един сървър губи 50% от стойността си вследствие на червей атакуващ неговата SQL база данни, тогава можем да кажем, че EF на такъв инцидент е 0.5.

За определяне на SLE можем да използваме следната формула:

стойност на актива x EF = SLE

Ако приемем, че общата стойност на актива на базата данни е 45 000 € и че EF за хакерска атака е 0.3, то SLE в този случай е 13 500 €.

Когато в процеса на оценката на риска взимат участие потребители, финансисти и IT специалисти, то значително по-лесно е SLE да се определя като се изхожда от необходимите средства за възстановяване на системата, отколкото чрез определяне на EF. Основната полза от използването на EF е, че той е винаги по-малък от единица и може да служи като коректив, когато са възприети нереални цени за възстановяване, т.е. при EF = 1, SLE на риска ще бъде цялата стойност на актива.

Сега, след като вече знаем SLE, можем да анализираме заплахата. Спомнете си, че заплахата по своята същност може да бъде човешка, природна или техническа. Заплахата поразява нашата система, като използва нейната уязвимост. Това, което трябва да определим е колко често очакваме, на годишна база, да сме подложени на специфична заплаха при положение, че не сме предприели мерки за противодействие. Тази стойност е известна като *годишна честота на реализация на риска (annualized rate of occurrence - ARO).* Стойност 0.0 означава, че през годината тази заплаха никога няма да се реализира. От друга страна стойност 1.0 означава, че е сигурно, че през годината дадената заплаха ще се възползва от уязвимостта един път. ARO = 0.1 показва, че заплахата се възползва от уязвимостта един път на 10 години, а пък ARO = 0.25 – един път на четири години.

Веднага се вижда, че даден риск може да се реализира повече от веднъж годишно. Инсталирането на операционна система в Интернет (с опции по подразбиране, без кръпки или използване на други механизми за сигурност) има продължителност на живота по малко от един ден, преди да стане жертва на нападение [3]. Означава ли това, че ARO трябва да бъде 365.0, тъй като сървърът потенциално би могъл да бъде компрометиран 365 пъти годишно? ARO е дефиниран като *честота*, с която даденото събитие ще се случва. Когато ARO < 1.0, тази честота е много подобна на вероятност. Разликата е, че максималната допустима стойност за вероятността е 1.0, което означава, че събитието със сигурност ще се случи. Експертите се различават в мненията си, дали използването в изчисленията на ARO със стойности над 1.0 е смислено. В края на краищата се предполага, че въведените защитни механизми в дискутираната по-горе операционна система ще я предпазят за време по-дълго от един ден. Използването на ARO > 1.0 може да доведе до невероятни оценки за стойността на понесените щети на годишна база. Приемайки, че очакването за единична загуба на компанията (във време и разходи за възстановяване на мрежата при злополука) е 50 000 €, ARO = 365.0 ще доведе до

годишна стойност от 18 250 000 €. Това не означава, че използването на такава сума за защита на операционната система ще бъде икономически ефективно. В такива случаи обикновено се правят изчисления с ARO = 1.0, и се приема, че ако не се похарчат пари за намаление на риска, трябва да се предвиди в бюджета поне 50 000 € за възстановяване, тъй като организацията ще усети реализация на този риск през годината.

Как се определя ARO? По същия начин както и очакването за единична загуба – чрез разговори с различни специалисти и анализ. За различните заплахи ARO могат да приемат различни стойности.

Комбинирайки честотата или вероятността за заплаха на годишна база с очакването за единична загуба, можем да изчислим *очакваната годишна загуба* (*annualized loss expectancy* - ALE), т.е.

ALE = SLE x ARO

Много компютърни системи могат да работят в продължение на години без хардуерно поражение, което да смути работата им. На базата на подаденото от производителя *средно време между отказите (mean time between failures - MTBF)* и въз основа на собствения ни опит можем да приемем например, че един сървър претърпява хардуерна повреда веднъж на три години. Прилагайки тези разсъждения, можем да сътворим следната таблица:

Актив	Заплаха	SLE €	ARO	ALE €
Сървър	Хакер	10 000	12.0	120 000
Сървър	Критичен хардуерен срив	16 000	0.33	5 280
Сървър	Природно бедствие - торнадо	45 000	0.01	450

Информацията, която се съдържа в нея, трябва да се използва за създаване на политика за сигурност. Трябва да изберем как да се справим с риска. Имаме три възможности – да намалим риска, да възложим на някого риска или да го приемем.

Понеже непрекъснатото възстановяване на сървъра до работното му състояние отнема много време и е свързано с високи разходи, то едва ли ще намерите застрахователна компания, която да поеме грижата за това. Следователно вашата компания трябва да предприеме мерки за намаляване на риска от хакерски атаки, използващи уязвимостта на вашия сървър.

Когато разглеждаме случая на критичен хардуерен срив, можем да приемем, че средното време за ремонт ще бъде сведено до минимум ако наблизо има склад за резервни части или дори готов сървър в състояние на „горещ резерв”. Срещу определена такса някои производители гарантират доставка на резервни части в рамките на четири часа. Заплащането на такава такса ще означава, че използваме метод за възлагане на риска от хардуерни повреди на трета страна. Създаването на собствен склад с резервни части е вече използване на друг метод - за намаляване на риска. Този метод използваме и когато поддържаме в готовност резервен сървър.

Поддържането в готовност на резервен сървър със сигурност ще струва повече от 5 280 € годишно, тъй като освен хардуера трябва да се поддържа и операционната система заедно с нейните кръпки съответстващи на базовите конфигурации на останалите сървъри; трябва да се поддържа документацията на различните приложни програми и т.н. Може да се окаже, че поддържането на такъв сървър е икономически изгодно само в случай, че той служи за резерва едновременно на 10 – 15 сървъра, изградени на една и съща платформа. Какво става, когато дружеството няма нужда да поддържа 10 – 15 сървъра? В този случай вероятно ще бъде взето решение, че с цел намаляване на риска е по-изгодно да се плаща премия за приоритетно обслужване на външен оператор.

И накрая, разглеждайки случая на природно бедствие, компанията най-вероятно ще приеме риска с разбирането, че ако ни удари торнадо, дружеството ще фалира и няма да има необходимост от възстановяване на сървъра.

Компанията може също да реши, че комбинацията от намаляване на риска и възлагането му на трета страна представлява икономически най-изгодното решение. Рискът от хакерски атаки може да бъде намален например с използване на *защитни стени (firewalls)*. По-нататък рискът може да бъде редуциран с прилагане на *ешелонирана защита (defense in depth)*, чрез добавяне на контрол за достъп до сървърите използващ *система за откриване на нарушители (intrusion detection system – IDS)*, като се използва *криптиране на чувствителните данни (encryption for sensitive data)* и т.н. Всяка една от тези мерки за противодействие намалява риска от хакерски заплахи. Предприемането на такива мерки може да бъде дълъг процес, като зад всяка мярка стои някой, който обмисля начините за нейното приложение. Вместо да се харчат все повече и повече средства за по-нататъшно намаляване на риска, може, при достигането на определен праг, останалата част от риска да се възложи на застрахователно дружество.

Прилагането на някои мерки за противодействие оказват въздействие върху няколко риска едновременно. Например една защитна стена за филтриране на пакети може потенциално да защити десетки системи. Когато обсъждаме мерките за противодействие, ние ще използваме ALE информацията, за да определим кои мерки са най-ефективни от технологична и икономическа гледна точка.

Основният недостатък на количествения анализ е, че въпреки точността му, той трудно може да бъде направен както трябва. Обикновено няма общо съгласие между производителите на оборудване и анализаторите на риска по отношение на видовете заплахи и честотата на тяхното появяване. Следователно ако нямаме голямо количество натрупани и анализирани достоверни данни, количествените резултати не са нищо друго, освен едно добро предположение на експертите. Друг сериозен недостатък е, че докато самите изчисления на количествения анализ са съвсем прости и ясни, процесът на събиране на данни е доста сложен и не достатъчно методологически изяснен. Ето защо много корпорации и експерти по сигурността разчитат на друг метод за оценка на риска, а именно на качествения анализ.

1.2.4.5 Качествен анализ на риска (Qualitative Risk Analysis)

Качественият анализ на риска използва опита и интуицията на тези, които най-добре познават активите на дружеството. Това означава, че хора с познания ще използват опита си за да оценят какви рискове заплашват активите и какви мерки да се предприемат срещу тях. Този метод има предимството, че е гъвкав и лесен за изпълнение.

Доверявайки се на опита на тези, които всекидневно работят с активите, може да се планира подходящ режима на приложение на ответните мерки.

Понеже качественият анализ в значителна степен зависи от преценката на хората, то той е по-ефективен когато повече специалисти участват в този процес. При прилагането на този метод могат да бъдат използвани въпросници с оценки от 1 до 10, интервюта, групови срещи, подробни хипотетични въпроси, и изобщо всяка техника, която позволява на хората да изразят своите становища по отношение на заплахите и намаляването на риска. На практика проучването на мнението на всеки човек, който е пряко заинтересован от използваната политика за сигурност е в полза на качествения анализ на риска. Ясно е, че група от компетентни лица може да идентифицира повече рискове и да предложи по-голяма гама от ефективни мерки за противодействие, отколкото един единствен човек.

Процесът на качественият анализ е подобен на процеса на количествения анализ, но в него не се използват числа и формули. Първо се идентифицират активите, които да бъдат защитавани. След това се прави мозъчна атака за определяне на потенциалните рискове, които заплашват всеки актив. Накрая групата решава кое е най-ефективното противодействие на всеки риск.

При качествения анализ изчисленията не са сложни, но и той от своя страна страда от редица недостатъци. Основният проблем при него е субективният характер на анализа и липсата на обективна информация за стойността на активите. Получените резултати могат да се променят в широки граници в зависимост от това, дали действителната стойност на актива е надценена или подценена. В някои отношения обаче, именно този недостатък прави качествения анализ по-популярен.

1.2.4.6 Комбиниране на количествения и качествения анализ на риска

В зависимост от организационната структура, управлението на корпорацията може да остане доволно от резултатите на качествения анализ. На някои организации обаче се налага да оправдаят техните разходи и затова те се нуждаят от информацията, която произвежда количествения анализ. На практика се използват елементи от двата анализа. При определянето на фактора за очаквано поражение EF и на очакването за единична загуба SLE в количествения анализ винаги присъства качествен елемент. Малко институции могат авторитетно да прогнозират, че EF не е 0.65 а 0.50 или че годишната честота на реализация на риска ARO е 0.3, а не 0.4. Тези числа се определят по-точно в процеса на дискусия с експертите, чиито мнения пък се определят от тяхната собствена интуиция и опит.

1.2.5 Избор на мерки за противодействие

До тук ние вече знаем какви са нашите мрежови активи. Имаме също добра представа за рисковете на които са подложени те, и колко ще ни струва, ако тези рискове се реализират. Сега е времето да определим какви стъпки да предприемем в защита на тези активи. Накратко, трябва да изберем мерки за противодействие. Използвайки терминологията на анализа на риска, мярка за противодействие е всяко нещо, което ефективно намалява вероятността за реализация на даден риск. Така предприетата мярка за противодействие трябва да намали или SLE или ARO. Тъй като средната ALE за всеки риск се основава на тези две стойности, всяко нещо, което намалява някоя от тях, ефективно ще намали и очакваната годишна загуба ALE.

Противодействието може да бъде техническо решение, но то също така може да бъде и административно или физическо решение. Помислете как някой може да се възползва от незаключената сървърна зала. Ефективното противодействие в този случай може да бъде просто едно физическо заключване. Ако ключалката и ключът не са достатъчни за да следим кой влиза и излиза от сървърното помещение, тогава може би ще трябва да се използва ключалка с биометрична идентификация. Това значително ще намали вероятността ключът да попадне в неподходящи ръце. Тук ние сме добавили технически елемент към нашето физическо решение. Ако това все още не е достатъчно, можем да приложим и допълнителни административни мерки, например въоръжена охрана при вратата.

Използването на нови технологии не е единственият избор. Когато хората употребяват термина *ешелонирана защита (defense in depth)* при обсъждане на въпросите на информационната сигурност, те нямат предвид използване една след друга в последователност на четири защитни стени. Те мислят и за административни и физически мерки за противодействие. В някои случаи тези мерки са по-евтини и по-ефективни, отколкото използването само на технически решения.

Избирайки мерки за противодействие, преминаваме вече към фазата на прилагане на нашата политика за сигурност. Анализът на риска ни е казал какво трябва да се защитава. Мерките за противодействие определят как точно нашите активи да се защитават. Това е стъпката, с която повечето хора започват, когато трябва да изградят план за защита. Избираме какво би било най-добрата инвестиция за защита на нашата мрежа.

При избора на противодействие, ние се ръководим от два елемента. Първо, ние искаме мярката за противодействие да има добра цена и нейното осъществяване да представлява добра бизнес сделка. Дали това е така установяваме, като правим *анализ на разходите и ползите (Cost/Benefit Analysis)*. Вторият елемент от който се интересуваме е функционалността и ефективността на нашите мерки за противодействие. Ако успеем да намерим две решения, които представляват ефективни мерки за противодействие на даден риск, и едновременно с това и двете решения са изгодни от бизнес гледна точка, то кое от тях да бъде предпочетено за приложение в нашата компания? Именно с тази тематика ще се занимаем в този раздел.

1.2.5.1 Анализ на разходите и ползите (Cost/Benefit Analysis)

Цялата извършена работа до този момент служи само за да ни позволи да направим критично важно решение – кои мерки за противодействие са най-смислени от бизнес гледна точка за сигурността на мрежата. От бизнес гледна точка означава, че цената на решението трябва да е по-малка от цената на проблема. Казано по друг начин, няма смисъл да похарчим 100 000 € на година, за да решим проблем, който би могъл да ни струва средно не повече от 50 000 € годишно. Това може да се изрази фигуративно с формулата:

$$V = B – A – C,$$

където V е стойността на мярката за противодействие, B е равно на ALE преди прилагането на мярката, A е равно на ALE след прилагане на мярката, а C е цената на самата мярка за противодействие.

Използвайки отново разгледания вече пример, ние знаем, че нашият сървър има ALE = 5280 € по отношение на критичен хардуерен срив. Нека приемем, че едно от решенията е да използваме непрекъсваемо токозахранващо устройство (Uninterrupted Power Supply – UPS), с което намаляваме стойността на ALE за този риск на 950 € годишно. Устройството UPS и резервните части, които поддържаме на склад за три години ни струват 2400 €. Следователно, годишно ние имаме разходи 2400/3 = 800 €. Това означава, че стойността на нашата мярка за противодействие е 5280 € - 950 € - 800 € = 3530 €.

Така, нашата мярка за противодействие ще добави стойност за компанията в размер на 3530 €. Тази стойност може да бъде сравнявана със стойностите, които други решения генерират. Например, ако друго решение, което би намалило риска от критичен хардуерен срив на сървъра е също така добро, но за него изчислим стойност от 4200 €, то лесно се вижда кое от двете решения ще бъде предпочетено, а именно това, което носи по-голяма стойност, или с други думи по голяма ***възвращаемост на инвестицията*** (*return on investment - ROI*) за нашата компания.

Понеже ALE вече е изчислено, то има два начина да влияем върху стойността на мярката за противодействие. Първият начин е да се влияе върху стойността на A във формулата. Една мярка може да намали A до 100 €, докато друга – само до 2 000 €. При равни други условия, тази мярка, която намалява най-много A ще бъде предпочетена. Например, ако това са две различни защитни стени, и едната намалява A до 100 €, а другата до 2 000 €, то изборът на първата защитна стена е по-добро решение. Това не означава, че първата защитна стена е по-бърза, с повече функции и т.н. Всъщност втората защитна стена може да се отличава с по-добро изпълнение, да има повече функции, но те да не са необходими за нашата мрежа. Тя може да струва и значително по-скъпо.

Вторият начин е да влияем на стойността C във формулата. При еднакво намаление на риска е по-разумно да бъде предпочетено решението, което е по-евтино. Когато определяме обаче цената на мярката за противодействие не трябва да вземем просто цената от фактурата за закупуване на оборудването. Тук се включва и обучението, конфигурирането, тестването, съвместимостта със съществуващите приложения и въздействието върху тях, изменение на пропускателната способност и т.н. Едно противодействие може да е евтино, но когато компанията открие, че вследствие на програмна несъвместимост производителността е намаляла с 2%, то това противодействие няма вече да е толкова атрактивно.

Има и редица други фактори, които трябва да се вземат предвид, при оценката на функционалността и ефективността на мерките за противодействие. По-долу са изброени някои от тях. Сравнението по списък като този може да бъде много полезно, особено когато се сравняват продукти на различни производители.

1.2.5.2 Различни фактори влияещи върху избора на мерките за противодействие

Одобрение на потребителите

Мярката за противодействие трябва да бъде в такъв вид, че да не е прекомерно натрапничава и да не затормозява потребителите на мрежата. Не би могло например да се използват ДНК проби в процеса на автентикация. Повечето хора ще се противопоставят на това. Одобрението на мярката от страна на потребителите е много важно. Ако нейното прилагане значително ги затруднява да извършват ефективно своята всекидневна работа, то те със сигурност ще намерят гениални начини да я заобиколят. Пример за неподходяща мярка може да бъде използване на случайно генерирана 16-знакова парола, която при това задължително трябва да се променя на всеки 10 дни. Повечето потребители не са в състояние да запомнят такива пароли и със сигурност ще ги запишат на лист хартия, пазейки ги на удобно за тях място.

Резултатите от изследването на одобрението на потребителите понякога са много интересни. Например при контрола на достъпа до мрежата с използване на биометрични данни, най-ефективните такива методи (като сканиране на ретината или на ириса) са най-малко популярни. Обратно, най-малко ефективните методи (като анализ на подписа и следене на натискането на клавишите) са сред най-одобряваните от страна на потребителите.

Влияние върху активите

Мярката за противодействие не трябва да оказва сериозно влияние върху ресурсите, които защитава. За класически пример могат да служат проблемите с които се сблъскваме в някои топологии при едновременното използване на NAT (network address translation) и IPSec. Използването на криптиране (в IPSec) води до нежелан ефект и промяна на актива, който се опитваме да защитаваме (NAT). За да осигурите едновременна работа на двете технологии е необходимо да се извършат инженерни промени, Това увеличава разходите за прилагане на мярката за противодействие, намалява нейната ефективност и въвежда допълнителна сложност, която от своя страна води до неизвестни последици за сигурността на мрежата.

Възможност за предупреждаване

Когато оценяваме възможността на определена мярка за противодействие да предупреди администраторите за случващо се събитие, трябва да вземем предвид два елемента. Първият от тях е начинът, по който това може да стане. Има ли устройството възможност да изпраща електронна поща? Какво става когато мрежата блокира? Може ли за това да се съобщи на администраторите по друг начин, например чрез набирането на телефонен номер и оставяне на съобщение. Другият елемент е възможността за настройка на самите предупредителни сигнали. Обикновено в първите няколко дни след инсталиране на мярката за противодействие всеки нов мрежов администратор се вълнува когато е уведомен за случващо се събитие. След осмият сигнал за тревога обаче това започва да му омръзва. Уверете се, че устройството има възможност за настройка да сигнализира за някои събития а други просто да ги регистрира. Най-добре е даже администраторът да бъде известяван само за критично важни събития. В края на краищата някои предупреждения са по-важни от други. Ако устройството няма такава възможност за

настройка, то трябва да очакваме, че след кратък период от време всички системи издаващи предупредителни сигнали ще бъдат изключени.

Одит

Мярката за противодействие трябва да позволява различни степени на одит. От една страна, когато проверяваме едно събитие или търсим определен вид дейност, ще ни бъде много от полза, ако разполагаме с подробни записи. От друга страна, когато всички записи са многословни, ние срещаме определени трудности при разпознаване чрез тях на конкретно събитие. Затова трябва да има възможност да се правят записи с минимална дължина при обичайните транзакции.

Възможност за възстановяване на първоначалната конфигурация

Мярката за противодействие трябва да може да бъде възстановявана до първоначалната си или до съхранена конфигурация. Възможността за бързо рестартиране на системата е важна при възникване на грешка в устройството. Използването на Microsoft Windows ни е научило вече, че рестартирането може да реши много проблеми. Ако администраторът забрави паролата си и няма възможност за нейното възстановяване, то единственият изход е връщане на системата в първоначалната и конфигурация от страна на производителя. Ето защо трябва да се провери дали устройствата, които възнамеряваме да използваме, имат възможности за възстановяване на административните пароли и до зареждане в тях на изпитани вече, работещи конфигурации.

Независимост на мярката за противодействие от актива, който защитава

В идеалния случай ние искаме да имаме възможност да премахнем или променим мярката за противодействие, без това да повлияе на защитавания актив. Това по-лесно може да се направи, ако противодействието е физически или логически отделено от актива. В този случай с една мярка можем да защитаваме множество различни системи. Да вземем за пример защитна стена. Вие можете да закупите една защитна стена и да я конфигурирате да защитава определен компютър (host-based firewall). В този случай тя ще защитава само компютъра за когото е конфигурирана. Ако решите да защитавате повече компютри, то трябва да изберете защитна стена като самостоятелно устройство. Това естествено ще увеличи не само разходите но и ползите. Ако се наложи промяна на стратегията, ще бъде сменена само защитната стена, без намеса в компютърните системи.

Сигурни състояния по подразбиране на устройствата

В желанието си да се харесат на потребителя, някои съвременни операционни системи се конфигурират по подразбиране като много несигурни. Разработчиците на приложения с право твърдят, че сигурността води до увеличаване на сложността на системата и затова обикновено те взимат решения, които фаворизират лекотата на използване пред сигурността. Ето защо при избора на мярка за противодействие, трябва да се спрем на такива продукти, за които параметрите по подразбиране ни осигуряват една в значителна степен защитена система. В примера със защитната стена това означава, че при липса на конфигурация или повреда в устройството, всякакъв трафик трябва да бъде абсолютно забранен. Това със сигурност няма да ни хареса когато се случи, но ако разгледаме алтернативата – произволен трафик да преминава по подразбиране, то ние няма да

разберем за повредата, защото нормалният ни трафик няма да бъде засегнат. Преминаването към защитено състояние (никакъв трафик) при повреда ще бъде забелязано обаче не само от нас, но и от хакерите, които ще разберат за повреда в защитната стена.

Зависимост от други компоненти

За да се гарантира правилното функциониране е необходима минимална зависимост от другите компоненти. Сложността се счита за враг на сигурността и мерките за противодействие, които разчитат на взаимодействие с други компоненти, трябва да се разглеждат като по-неудачни в сравнение с мерките които функционират независимо от останалите. Това не означава, че такива мерки не могат да бъдат прилагани – понякога те не могат да бъдат избегнати. Централната станция за регистриране не би могла да изпълнява своите функции, ако не получава съобщения за регистриране от отдалечените станции. Трябва само да имаме предвид, че когато сравняваме два еквивалентни продукта, ще се отдаде предпочитание на този, който функционира значително по-независимо.

Различни нива на достъп

Основният критерий тук е да съществува ясно разграничаване на правата за достъп на потребителите и администраторите. Това ни гарантира възможността за одит на достъпа до устройството. В идеалния случай трябва да има възможност на всеки потребител да се приписват административни функции, вместо да се използва един единствен административен акаунт. Помислете си за объркването, което ще възникне, ако някой влезе в устройството в 9:00 часа като „администратор" и започне да прави промени. Ако има четирима човека в организацията които знаят паролата, трудно ще се разбере кой е направил промените, особено ако паролата е научена с хакерска атака или човекът умело затрива следите си. Ако знаем конкретно потребителското име на този, който е влязъл с административни функции и е извършил промените, то ние можем лесно да променим неговия профил (като забраним достъпа му) или да наложим административни наказания.

Гъвкавост и функционалност

Въпреки че основната ни цел при избора на продукт е той да бъде функционален и ефективен, ние трябва да бъдем загрижени също така и продуктът да притежава определена гъвкавост. Трябва да проверим какви опции за конфигуриране той поддържа. Например, ако даваме оценка на VPN устройство, то какви протоколи за кодиране са възможни? Какви IPSec режими могат да бъдат конфигурирани? Като потребител трябва да можете да разрешите само опциите, които са необходими, и да забраните онези, които не трябват. Не се радвайте на графичния интерфейс. Използването на графичен интерфейс обикновено затруднява смяната на конфигурацията. Помислете как ще взаимодействате с устройството. Трябва ли конфигурирането да се извършва винаги през конзолата, закачена към серийния порт, или може това да стане от разстояние, по мрежата? Има ли начин за дистанционно управление на устройството? Ако такъв начин съществува, то как е гарантирана сигурността на самата сесия? Интерфейсът за управление представлява ли значителен риск сам по себе си и какви алтернативи за връзка имате?

Функционалността и гъвкавостта на устройството, както по отношение на вариантите за конфигуриране, така и по възможностите за управлението му, оказват значително влияние върху обучението и оперативните разходи свързани с това устройство.

Изисквания за минимална човешка намеса

В процеса на конфигуриране хората правят грешки и създават нови уязвимости. При сравняване на ефективността на мерките за противодействие, помислете за размера на конфигурационния файл, който е необходим за дадено устройство да функционира както трябва. В идеалния случай бихме искали мерките за противодействие да са колкото е възможно повече “plug and play” и да имаме минимална човешка намеса в съществуващото обкръжение.

Модулност

Помислете за мерки за противодействие, които са модулни по своята природа; те са по-добри от онези, които не са модулни. Това качество ще ни позволи да инсталираме или премахваме мерки за противодействие с минимално въздействие върху нашите активи или върху други мерки. Модулната природа обикновено увеличава функционалността и гъвкавостта на устройството. Да разгледаме защитна стена, която има и модули за сканиране на електронната поща за вируси и сканиране на трафик за съмнително съдържание. Макар че не всички тези функции могат да се изискват от нашата политика за сигурност, то възможността да ги добавите в бъдеще или да ги разрешите, когато е необходимо, може да намали разходите и да позволи на администраторите гъвкаво да конфигурират такива мерки, каквито са необходими за мрежата в момента.

Лесно разбираем изход

Хората трябва да могат да използват информацията, която мярката за противодействие произвежда. Независимо дали това е по време на отстраняване на проблеми, при одит или настройка на устройството. Резултатът, който може да се чете от хората без специално обучение е много по ценен от информацията, която например е в шестнадесетичен вид. Ние също бихме искали тази информация да е под формата на отчети, които да ни дават възможност за задълбочен технически анализ. Желателно е тези отчети да могат да бъдат модифицирани и обобщавани за да служат като справки за ръководството. Много производители, в желанието си да предразположат потребителя към техния продукт, включват като изход отчети с изчертани цветни графики. Не това е най-важното – просто се уверете, че нужната за вас информация присъства и че имате възможност лесно да я персонализирате.

Ако хората са объркани и уплашени от техните мрежови инструменти, то инструментите никога няма да бъдат използвани с пълния си потенциал. Повечето компании ще предпочетат да използват продукти, които произвеждат разбираем изход, пред такива, които изискват допълнителни разходи за обучение и усвояване, за да разберем в края на краищата какво дадения инструмент ни казва.

Сигурност на устройството

Понеже нашата цел е подобрението на сигурността на мрежата чрез избор на мерки за противодействие, то ние трябва да сме сигурни, че самата мярка, като такава, не внася допълнителна уязвимост. Това включва как да реализираме сигурен достъп до устройството. Ако използваме уеб сървър за нуждите на уеб базирано управление, то има ли този уеб сървър някаква уязвимост? Как е криптирана комуникацията с устройството? Каква автентикация на потребителите използваме? Почти винаги ние знаем предварително уязвимостта на устройствата които поръчваме. Ако пък открием уязвимост на устройството, която не ни е била известна, то трябва да се обърнем към производителя за съдействие. Производителят трябва да разработи и да ни предостави необходимите кръпки за фирмуера.

Една от най-лошите ситуации, с които се сблъсква мрежовият администратор е, когато се открие уязвимост, или се появи публикация за подобно събитие, а той няма на разположение необходимите кръпки за преодоляване на тази уязвимост. Веднага след като уязвимостта е станала публично достояние, много хакери ще създадат автоматични заплахи за да експлоатират този недостатък. Те ще създадат скриптове или просто ще включат тази заплаха в следващия вариант на разпространяващите се в Интернет заплахи от вируси, червеи и троянски коне.

Производителност на системата

Някои мерки за противодействие могат да окажат неблагоприятно въздействие върху производителността на вашите активи. Класическият пример е IPSec VPN. Поради сложния процес на криптиране и декриптиране на данните в двата края на канала мрежовата производителност значително намалява. Освен това VPN устройството в даден момент от време поддържа само ограничен брой сесии. Използването на „интелигентни" защитни стени създава допълнителни закъснения в мрежата. При сравняване на мерките за противодействие трябва да вземете предвид и вероятните натоварвания на защитните стени. Ако имате 500 служители, които очакват да използват VPN в нормалната си работа, вашата система трябва така да е проектирана, че да поддържа в пиков момент значително повече едновременни връзки. Ако вашата защитна стена няма функции само да филтрира пакети, но ще сканира също електронната поща за вируси и уеб страниците за съмнително съдържание, както и ще служи като прокси сървър за 1000 служители, трябва да направите много внимателен преглед на техническите спецификации на производителя.

Повече от тези проблеми могат да бъдат решени чрез използване на по-мощни процесори, по-големи и по-бързи твърди дискове и повече системна памет. Това разбира се ще увеличи разходите и ще се отрази при анализа на разходите и ползите.

Възможност за надграждане

Мярката за противодействие трябва да има възможност за надграждане и разширение. Често компаниите се опитват да спасят няколко евро в краткосрочен план и закупуват хардуер, който е с ограничени възможности за разширение. Не след дълго те откриват, че изискванията за сигурност на тяхната мрежа растат с течение на времето. Закупуването на устройства, които позволяват разширяване, е малко по-скъпо първоначално, но в

дългосрочен план по този начин се предотвратява неизбежната пълна подмяна на устройствата.

Възможност за тестване

Защитата, която предлага мярката за противодействие, трябва да може да бъде проверена и тествана, т.е. да има възможност за „одит”. Търсим такива решения, при които лесно можем да видим обратната връзка от защитата, т.е. да се убедим в нейната ефективност. Това от една страна ще позволи на администратора да спи спокойно нощем, а от друга страна ръководството ще бъде щастливо, че е изхарчило парите си разумно.

1.2.5.3 Административни мерки за противодействие

Както вече беше споменато, не всички мерки за противодействие трябва да бъдат технически. Истинската неизвестна величина за сигурността на мрежата все пак са хората, а не техниката. Най-добре е да се създаде политика за сигурност, която защитава информацията по много различни начини. В този раздел накратко ще бъдат представени административни мерки за противодействие, които могат да се използват за повишаване на сигурността на мрежата.

Административният контрол трябва да бъде разглеждан като най-високо ниво в политиката за защита на информацията. Неговото съществуване създава очаквания за използваните технологии, съоръжения и поведение по отношение на информационната сигурност. Административният контрол включва такива неща като контрол на персонала, обучение за осигуряване на сигурността, тестването и надзора, както и други политики и процедури, свързани с административни задачи.

Контролът на персонала включва процедури, които управляват взаимодействието на служителите и са адресиране към всякакви въпроси свързани с неспазването на определените правила. Най-често срещания пример за проверка на персонала са одобрените политики за ползване (acceptable use policies -AUPs), които описват в детайли правилната употреба на мрежовите ресурси и последствията от нарушаването на определената политика.

Контролът на персонала обикновено се опитва да намали риска в мрежата чрез контролиране на работната среда. Един от начините да се направи това, е да се наложи строго *разпределение на отговорностите (separation of duties)* по отношение на критични бизнес функции. Например в много компании мрежовите администратори изпълняват всички функции в мрежата, от поддържане на мрежовата сигурност и оказване на техническа подкрепа на потребителите, до конфигуриране на приложения. Не е трудно да се забележи в колко деликатно положение е поставена такава компания. Администраторът има не само пълен достъп да мрежата, но той не е подложен и на никакви външни проверки. Всяко действие което предприеме мрежовия администратор може да бъде прикрито от същия този администратор. Той може да използва компютърните ресурси и свободния капацитет на мрежата за свои собствени бизнес цели. Очевидно това е неприемливо.

Преди да започнете да подозирате вашия мрежов администратор, трябва да знаете, че повечето мрежови администратори са съзнателни и работливи хора, които обикновено са

претоварени и недооценени. За тях забравяме когато нещата вървят добре, но когато положението се влоши, те са първите посочени като виновни.

Когато е възможно, политиката по сигурността на информацията трябва да включва разпределение на отговорностите по отношение на важните ресурси на компанията. Едно такова разпределение предвижда съществуването на три главни функционални роли: администратор по мрежова сигурност, оперативен администратор и администратор за крайните потребители.

Администраторът по мрежова сигурност прилага политиката по сигурността, прави преглед на дневниците, проверява всички събития и отговаря за компютърните инциденти. Оперативният администратор се грижи сървърите и мрежовите устройства да работят правилно, поддържа приложенията и софтуерните кръпки на операционните системи на сървърите. И накрая, администраторът за крайните потребители носи отговорност тези потребители да имат съответните права, за да изпълняват своите служебни задължения.

Контролът на персонала може също да включва и въпроса за ротация на задълженията. Използвайки горния пример на разпределение на отговорностите, периодично, трите мрежови администратори могат да заменят своите функции. Това носи осезаеми ползи за информационната сигурност. Първата голяма полза е, че се насърчава обучението на администраторите. Ако някой от тях отсъства поради някаква причина, то в критични ситуации разполагаме с подготвен човек, който да го замести. Втората полза е, че става много по-трудно да се прикрият неподходящи действия, когато имаме ротация на отговорностите.

Все пак трябва да отбележим, че комбинацията от разпределение на отговорностите и тяхната ротация намалява, но не елиминира напълно възможността администраторите да се споразумеят да извършват заедно незаконни или измамни дейности.

Прилагането на политиката за сигурност може да бъде много трудна битка, ако крайните потребители не са подходящо обучени как да прилагат методите за сигурност в тяхната всекидневна работа, и не разбират необходимостта от информационна сигурност. Когато очакваме потребителите да взаимодействат с елементите по сигурността, те трябва да бъдат адекватно обучени не само как да изпълняват задачите си, но и да разбират мотивите движещи тяхната дейност. Да разгледаме един прост пример, който често се среща – политиката за използване на пароли. Вместо просто да наложим политика, която изисква паролите да имат 10 знака, някои от които да са букви, а други цифри и с това да смятаме, че въпросът е решен, то потребителите могат да бъдат инструктирани *защо* е важно да се използват сложни пароли, а след това да ги научим *как* да генерират пароли които да отговарят на дадената политика и едновременно с това все още да могат да ги помнят. Административният контрол в този случай следва да включва процедура свързана с обучението на потребителите в мрежата.

Макар че самите потребители могат да представляват заплаха за сигурността на мрежата, в повечето случаи това не се дължи на тяхната злонамереност. От потребителите се очаква определена производителност, и за да я постигнат, те могат да бъдат невероятно изобретателни в заобикалянето на политиката за сигурност, когато разберат, че тя им пречи да си свършат работата в срок. Това не може да се промени само с административни забрани, но такива забрани могат да служат като начало.

Административният контрол следва да създаде и методи за напомняне на потребителите за ползите от информационна сигурност, за показване на предимствата, и за награждаване при постоянно поддържане на мрежата сигурна. Малко искрена благодарност и признание може в значителна степен да мотивира хората позитивно.

Цялата политика за сигурност на информацията трябва да се проверява от време на време. Това се прави за да сме убедени, че политиката все още е уместна и подходяща, и че гарантира това ниво на защита, което създателите на тази политика са очаквали от нея.

И накрая, административният контрол включва персоналната йерархия на организацията. Това е важен елемент в процеса на търсене на отговорност при нарушение на политиката за сигурност. Ръководителите трябва да са пряко отговорни за действията на подчинените си.

Административният контрол е добра илюстрация на това, че само техниката няма да бъде достатъчна за защита на вашата мрежа. Ние можем да идентифицираме потребителите с пароли, но ако те генерират лоши пароли или ги записват, какво наистина постигаме? Ние можем да кодираме счетоводни файлове с използване на методи за силна криптография, но ако счетоводителят споделя тези файлове с приятеля си в областта на маркетинга, то нашето кодиране не е компрометирано, но нашата политика за сигурността е. Всяко техническо решение което се предлага следва да бъде придружено с подходящ административен контрол, разбира се когато това е уместно.

1.2.5.4 Физически мерки за противодействие

Физическите мерки за противодействие се разглеждат в съвсем отделна дисциплина на информационната сигурност. Тук ще представим само някои препоръки от най-високо ниво, които да се имат предвид при защитата на мрежата.

Когато разглеждаме техническите мерки за противодействие, ние често разсъждаваме върху защитата на периметъра на нашата мрежа от пакетни (packet-based) атаки. Това означава, че има някои „лоши" пакети извън нашата мрежа, които ние се стараем да не ги допуснем вътре. Обикновено се използват защитни стени, които да спрат тези „лоши" пакети. Физическата сигурност използва същия подход, но вместо да се занимава с пакети, държи далеко от нашата мрежа „лоши" хора или други заплахи.

Това може да стане по много различни начини - като използваме ключалки, катинари, вериги, камери и охраняващ персонал. Всички те попадат в категорията контрол на периметъра. Използването на такива средства води до намаляване на риска някой да получи физически достъп до нашите ресурси. Тези мерки не гарантират сигурността на съоръженията, но значително могат да забавят нарушителя.

Ние можем да приложим и строг контрол на движение на персонала в периметъра на нашата мрежа. Функционалните области на мрежата обикновено са отделени една от друга. Мрежата за изследвания и развитие, например, физически е отделена от административната мрежа и от мрежата на останалите потребители. Тя използва физически различни комутатори, достъпът до които е през защитна стена, или пък това е напълно отделна физическа мрежа, със своя собствена демилитаризирана зона (DMZ) и

глобални връзки които са конфигурирани да отговарят на специфичните изисквания предявявани към този тип мрежи.

При архивирането на данните също трябва да бъде упражнен физически контрол. Архивираните данни трябва да се съхраняват извън залата на сървърите, в заключено помещение, което има специална противопожарна защита. Осигуряването на физическата неприкосновеност на архивите със сигурност може да бъде определено като физически контрол.

Само служители на даден отдел трябва да имат достъп до работните станции разположени в този отдел. Физически контрол трябва да се осъществя и върху самите работни места – всички флопи и CD устройства трябва да бъдат отстранени, USB портовете да бъдат изключени и изобщо да няма никаква възможност за работа със сменяеми носители. Личният багаж на персонала понякога също се налага да бъде проверяван.

1.2.5.5 Технически мерки за противодействие

Това, с което повечето експерти се занимават (с изключение на експертите по физическа сигурност), е използването на технически мерки за противодействие. Макар че тези мерки са малка част от цялостната схема за защита, те обикновено са най-чужди и смущаващи широката публика. Обикновено се смята, че са разбираеми само за ограничен кръг тесни специалисти по мрежови технологии. Това съвсем не е така. Техническите мерки включват ограничаване на достъпа до мрежата, създаване на сигурна мрежова архитектура, използване на криптиране, както и извършване на одит на всички по-горе изброени мерки за противодействие. По-късно ще разгледаме подробно само една от тези мерки , а именно системата за откриване на нарушители (Intrusion Detection System - IDS).

1.2.6 Създаване на документация за стандарти и процедури по сигурността

Знаейки вече какви мерки за противодействие ще бъдат ефективни, можем за започнем процеса на създаване на документите засягащи използваните стандарти и процедури. Тези документи просто описват какви технологии, административни процедури и физически контрол ще бъдат приложени, за да се подкрепи избраната политика за сигурност. Докато политическата декларация е обща, то тук е мястото където да се разискват такива технологии като IPSec, защитни стени, системи за откриване на нарушители, процедури за назначавания и уволнявания, стандарти за екологичен контрол и т.н. Тези документи могат да бъдат в подобен на политическата декларация формат, но трябва да описват какви конкретни стъпки е необходимо да бъдат предприети, за да се наложи политическия документ.

1.2.7 Създаване на ръководства за конфигуриране

Една от целите и предимствата на политиката за сигурност е прилагането на последователна политика в цялата организация. Целта на документацията за конфигуриране е тя да служи като настолно ръководство на органите за управление на информационната сигурност. Тази документация може да бъде много полезна и при разработване в бъдеще на допълнителни елементи на политиката за сигурност. Ръководствата за конфигуриране са предназначени за всеки служител който отговаря за

практическото прилагане на политиката за сигурност. В тях са описани списъците за достъп (access lists), конфигурационните опции на IPSec сесиите, разрешените услуги на сървърите, както и правата на създадените групи и на отделните потребители. Обикновено с този „документ" завършва поредицата от документи описващи мерките за противодействие (технически, физически и административни) прилагани в организацията.

1.2.8 Примери за стандарти по сигурността

1.2.8.1 Стандарти за паролите

Поверителният характер на информацията е от изключителна важност в модела на управление на бизнеса. За да се осигури този поверителен характер, всички пароли трябва да отговарят на следните изисквания:

- да са с дължина не по-малко от осем знака.
- да съдържат комбинация от големи (A-Z) и малки (a-z) букви на латинската азбука
- да съдържат поне една цифра или някой от знаците ~!@#$%^&*(){}[]:";'<>?,./\|
- да не са думи от някой език или употребяван жаргон
- никога да не бъдат записвани.

1.2.8.2 Стандарти за маршрутизаторите

Маршрутизаторите играят критична роля в процеса на предаване на информация в мрежата. Тяхната конфигурация влияе на поверителността, интегритета и наличността на информационните активи. Всички свързвания към маршрутизаторите трябва да стават с използване на потребителско име (username) и автентикация с RADIUS. В критични моменти или когато RADIUS системата не работи, локално свързване към маршрутизатор може да става само с потребителско име и парола на авторизиран за дадения маршрутизатор администратор. Изисквания към маршрутизаторите:

- Всички пароли в дадения маршрутизатор да се пазят кодирани.
- Всички услуги, които не са необходими за препращането на пакетите и за нуждите на регистрирането трябва да бъдат забранени. Ето някои конфигурационни команди забраняващи ненужни услуги на Cisco маршрутизатор:
  - #(config-if) no ip directed-broadcast
  - #(config) no service tcp-small-servers
  - #(config-if) no service udp-small-servers
  - #(config) no ip source-route
  - #(config) no ip http server
- В процеса на свързване с маршрутизатор, последният трябва да издава съобщение UNAUTHORIZED USE PROHIBITED. Това съобщение предупреждава, че всички действия с маршрутизатора се наблюдават и че неупълномощените лица няма да

получат информация за производителя, модела, версията на софтуера или положението на маршрутизатора в мрежата.

- Свързването с маршрутизатора е разрешено само в криптирани сесии. Използването но Telnet е забранено.

Създаването на политиката за сигурност, с описаните по-горе нейни документи, не е лесна задача. Идентифицирането на активите, извършването на анализа на риска и избора на съответните мерки за противодействие е трудоемко. За да бъде извършена тази работа добре, е необходимо да отделите време, да положите усилия и да включите в процеса много хора от вашата компания. Сама по себе си, политиката за сигурност не увеличава сигурността на мрежата – това в края на краищата са само думи. Независимо от това, използването на политика за сигурност е най-добрия начин да гарантирате, че в процеса на създаване на сигурна мрежа ще постигнете своите цели и ще намалите риска.

2. Системи за откриване на нарушители (Intrusion Detection Systems)

2.1 Общ преглед

Целта на защитната стена в мрежата е точно дефинирана. Тя предпазва една част от мрежата от друга нейна част, като разрешава или забранява определен трафик на базата на редица избрани критерии. По отношение на сигурността обаче винаги имаме определени съмнения. Откъде знаем, дали защитната стена изпълнява нейните функции? Как да разберем, че защитната стена е конфигурирана правилно? Сигурни ли сме, че през нея не преминава трафик от кибернетични атаки, които не са били предвидени, когато за първи път сме я конфигурирали? Устройството, което е проектирано да ни отговори на тези въпроси се нарича *система за откриване на нарушители (IDS - Intrusion Detection System)*.

Ако защитната стена е ключалката на вашата врата, то IDS е алармата срещу проникване с взлом. Защитната стена е мрежовия елемент осигуряващ защитата. В случай че защитата е преодоляна, IDS включва алармата.

Това, което IDS се опитва да прави, е оценка на всеки от милионите пакети които наблюдава в режим на нормална работа. За всеки пакет, който се разглежда, логиката на IDS определя дали пакетът е „добър” (с други думи такъв, какъвто нормално се среща в мрежата) или „лош” пакет. В този случай „лош” може да означава виртуално всякакъв, но обикновено се приема, че това е пакет, който независимо поради какви причини, не трябва да се среща в мрежата. Това дори може да означава, че пакетът нормално е „добър”, но е видян в „лошо” време.

Дейностите, които IDS предприема, когато види добър или лош пакет могат да бъдат най-различни. Понеже предполагаме, че голяма част от трафика в мрежата е добър, нормално IDS обръща внимание само на лошите пакети. IDS може да избере да игнорира напълно лошия пакет, да регистрира този пакет в дневника като предложение за по-късен анализ от страна на администратора, или да включи аларма и да извести всички определени за целта лица, че такъв пакет е открит в мрежата.

Определянето на това, какво е „добър” и „лош” пакет е обект на безкрайни дискусии и множество патенти и продукти. За да разберем какъв избор трябва да направим при

разделянето на добрите от лошите пакети, нека се опитаме да създадем своя собствена IDS.

В основата си, една IDS не е нищо повече от програма специално обучена да разпознава пакети (sniffer). Тази програма наблюдава преносната среда и записва всички пакети за допълнителен анализ. Засега ние ще разглеждаме IDS като прост анализатор на пакети. Къде да бъде той поместен в мрежата, за да бъде максимално ефективен, с това ще се занимаем по-нататък. На този етап ние ще включим нашата IDS към някой концентратор.

Като начало, ние прихващаме всички пакети от преносната среда и ги записваме в дневник (log). След няколко дни ще забележим, че разполагаме с гигабайтов файл съдържащ текстови данни, който трябва да бъде сортиран. За да си улесним работата, ще се опитаме да филтрираме данните в известна степен. Това можем да направим по няколко начина. Първото нещо което ни идва на ум е да въведем всички видове „добри" пакети. Няма да направим и няколко крачки и ще осъзнаем, че съществува голямо разнообразие от много и различни видове добри пакети. Затова трябва бързо да променим курса. Трябва да се опитаме да намерим някакви отличителни характеристики на лошите пакети, като направим преглед на специализираната литература и наличната информация за различните видове мрежови атаки. За всяка атака, за която намерим информация, създаваме съответен филтър на нашата IDS. Например ако сме сигурни, че никога в нашата мрежа не трябва да се появяват пакети с IP адрес на източника 0.0.0.0, ние създаваме съответен филтър и причисляваме такива пакети към лошите.

Въпреки че такъв подход може да отнеме много време, все пак броят на видовете лоши пакети е значително по-малък от броя на видовете добри пакети. Доволни от работата си, ние инсталираме нашата IDS и я включваме. Веднага ще забележим, че нещо не е в ред. IDS ни алармира за голямо количество „лоши" пакети, макар че работим в идеални условия, в мрежа, която не е подложена на атаки. Започваме да търсим източника на тези лоши пакети. Ще открием, че много от тях удивително приличат на добрите пакети, които използваме в нашата мрежа. За да отстраним проблема, ние прекарваме дни и седмици в настройка на нашата IDS. Всеки път когато открием лоши пакети ние извършваме разследване дали тези пакети са наистина лоши, или са част от нормалния трафик на мрежата. С течение на времето ентусиазмът ни за чисто нова IDS започва да намалява. Можем дори, поради непрекъснатия тормоз от фалшиви лоши пакети, да вземем решението за цялостно изключване на алармената система.

Ако все пак до това не се стигне и ние упорито продължим работата си по създаване на нови филтри в нашата IDS, в определен момент ща забележим, че броят на фалшивите сигнали драстично намалява. Това е, което ни доставя удоволствие от нашата работа, и ние най-вероятно ще продължим да добавяме нови и нови правила за нашата IDS.

Това щастие ще продължи до момента, когато с ужас разберем, че нашата защита е била разбита, и че имаме инсталирани троянски коне върху сървърите. Тогава ще започнем процеса на възстановяване на всичко от последния добър архив с който разполагаме, но понеже не знаем кога е извършена атаката, най-вероятно ще трябва да възстановим системата от оригиналните носители. Това е депресиращ процес. Ще си задаваме въпроса къде сгрешихме? Нашата защитна стена работеше, а IDS не ни алармира за лоши пакети. Едва на следващия ден ще открием, че е измислена нова атака, и че последствията от нея са точно такива, каквито ние сме открили при себе си. Затова трябва стриктно да следваме политиката непрекъснато да инсталираме новите правила

за откриване на атаки. Проблемът е, че ние можем да сваляме тези правила от сайтовете на специализираните фирми по сигурността, но тази информация ще дойде при нас, когато може би вече е твърде късно за нашата мрежа.

До тук ние научихме по трудния начин, че така изградената наша IDS страда от голям недостатък. Ако в системата не сме въвели информация за определен вид атака, то системата няма да ни сигнализира за нейната наличност. По същество нашата IDS е реактивна. Ние знаем само за атаки с които някой друг е бил нападнат, той е забелязал това и е известил Интернет общността за случката.

Можем ли да използваме друг подход? Например вместо да мислим за поведението на добрите и лошите пакети, да помислим за поведението на потребителите. Идеята е, че обикновените потребители са доста предсказуеми. Те използват мрежата по един и същи начин всеки ден. Сървърите ни са едни и същи. При предишния си опит за създаване на IDS ние научихме, че в нашата мрежа има неща, които се случват постоянно. Затова решаваме да категоризираме потребителския трафик като „нормален" и „ненормален". Задачите, които потребителите и мрежовите компютри изпълняват непрекъснато определяме като „нормални". Трафикът, който не е част от „нормална" задача се счита за „ненормален". Този вид трафик генерира аларми и се записва в дневника.

Основният момент при този подход е, че вместо да преминаваме през трудния процес на регистрация на нормалния и ненормален трафик, след което да го въвеждаме в IDS, ние позволяваме на IDS сама да научи кое е нормално и ненормално. Чрез наблюдение на трафика, ние можем да предскажем статистически какъв вид трафик се очаква между всеки две устройства в мрежата. Колкото повече наблюдаваме, толкова по-точни са нашите оценки. За ограничаване на настройките, които трябва да направим, ние дефинираме като нормален за IDS малък набор от възможности. Това означава, че даваме на IDS свобода на преценка какво е нормално и какво не. Не е необходимо когато потребителите направят нещо малко по-различно, веднага да се събира групата по сигурността. Това което се счита за нормално всъщност е малък прозорец на поведение на двете страни, който се определя статистически от IDS.

Този подход може да ни защити в бъдеще от нови атаки. Както може да се предполага, новата атака ще използва специфичен, различен вид трафик, който не е бил използван досега. Следователно той няма да бъде част от базата данни с образци на нормален мрежов трафик, ще бъде регистриран като ненормален и ще задейства алармената система.

Така че след инсталирането и конфигурирането на новия тип IDS, ние сме уверени в своята възможност да откриваме нови атаки срещу мрежата ни и да им противодействаме. Това е така докато не проведем сериозен разговор с експерт по сигурността. Той ще ни убеди, че нашите определения за нормалност и ненормалност са въз основа на наблюдаваното поведение на мрежовия трафик. Има две причини, които трябва да ни накарат сериозно да се замислим. Първата от тях е, как да разберем, че нашата мрежа действително не е била атакувана преди да сме инсталирали IDS? Трафикът от такива атаки би могъл да се счита вече за нормален. Освен това, кое ни гарантира, че някой няма постепенно и много внимателно да променя вида на трафика, така че да тренира IDS да не разпознава тези изменения като ненормален трафик. Ако поведението се променя достатъчно бавно, то трафикът винаги ще бъде разпознаван като нормален. Такива атаки биха останали напълно незабелязани от новата ни система.

С други думи трябва да си припомним основното правило на сигурността – няма перфектно решение. Дайте ми време, пари и мотивация, и всяка система за сигурност може да бъде компрометирана.

Можем да започнем да мислим за евентуално комбиниране на елементи от двата изложени до тук подхода. Да отбележим, че повечето атаки се основават на незаконно използване на мрежови протоколи. Например, нормално няма да видите URL GET заявка (заявка за уеб страница), която да съдържа дълъг низ от ../../../../ в нея. Това може да се получи, когато някой се опитва да достигне до определена директория, като премине през множество други. Ако се върнем към нашата оригинална идея и просто дефинираме всички нормални начини, по които искаме протокола да действа, то можем да заключим, че появата на горната форма е необичайно поведение и представлява някакъв вид атака.

Тъй като има много големи различия в протоколите, трябва да се обърнем към писмените стандарти на протоколните правила. Трябва да научим IDS какво представляват нормалните операции на даден протокол съгласно RFC документа и да конфигурираме системата да ни предупреждава за всички пакети които нарушават това поведение. Веднага след инсталирането на нова IDS, ние ще бъдем засипани от множество алармени сигнали от всякакъв вид. При това нашата мрежа не е изложена на атака в този момент. Естествено трябва да предвидим определен период за настройка към спецификата на конкретната мрежа, но количеството на алармите които получаваме почти винаги значително надхвърля очакванията ни.

Системите за откриване на нарушители, които в момента съществуват, са несъвършени и много често са непълни. Нито един модел на функциониране на IDS не е в състояние да открие всички атаки. Тези системи изискват значителни ресурси при първоначалното инсталиране и настройка. Независимо от продукта и начина, по който той се опитва да открие атаките, такава система винаги ще се нуждае от определен обучителен период за разпознаване на специфичните нужди на мрежата. Въпреки недостатъците, тези устройства са основен инструмент в модерните мрежи и спадат към някой от видовете, описани подробно по-долу.

2.2 Видове IDS

2.2.1 Съдържателно претърсващи IDS (Signature-Based IDS)

Това са едни от най-разпространените IDS. При тях образци на пакети, с които са направени опити за атака, се въвеждат в базата данни на IDS, след което IDS проверява дали всеки новооткрит пакет съвпада с някой от въведените й в базата данни образци. Пакетите, които съвпадат с образците, се маркират за по-нататъшна проверка. Този вид IDS е широко разпространен, разбираем и лесно се имплементира. Той обаче страда от два недостатъка: липса на информация за определена атака и липса на образци на пакетите от такава атака. Тези недостатъци произхождат от начина, по който IDS работи. За да се открие определен вид атака някой трябва да положи усилия и да премине през процедурата за дефиниране как тази атака изглежда и през процедурата за конфигуриране на IDS с тази информация. Разбира се, никой не може да знае как една атака изглежда, докато някой не е бил атакуван, не е открил атаката по някакъв начин, и не е информирал Интернет обществото за нея. Този процес на неизвестност може да трае от няколко часа до няколко дни след реализиране на атаката, в зависимост от това какво

е естеството на атаката, нейния обхват, както и какво внимание обръщаме на този проблем. Обикновено на атаките които нанасят големи поражения и са с широк параметър на действие се обръща по-голямо внимание и те се обработват по-бързо. Това едва ли е някаква утеха, тъй като вашата мрежа често е подложена на такъв тип атаки.

Броят на актуализациите на базата данни също трябва да се има предвид. Някои компании имат образци от всяка регистрирана в Интернет атака. Размерът на базата данни непрекъснато нараства. Въпреки че това звучи положително, то забавя действието на IDS. В другия край на спектъра са компании, които ползват малко подмножество от образци на „най-често срещаните" в Интернет атаки. Това подмножество обикновено ви защитава само от елементарните, скриптови атаки. По-рафинираните ще останат незабелязани във вашата мрежа. В идеалния случай можем да използваме един компромис между двете крайности. Въпреки наличието на голям набор от образци, ние можем да изградим библиотека и да включим в нея само специфични за нашите нужди образци. Там могат да присъстват например образци от атаки от типа отказ на услуга, но не и на атаки срещу FTP сървър, понеже ние нямаме такъв сървър в нашата мрежа. Ще инсталираме и конфигурираме само тези правила, които имат някакво отношение към нашето мрежово обкръжение.

Когато сравняваме продуктите от този вид IDS на различни контрагенти е особено важно да се разгледа и въпроса колко бързо даден контрагент реагира на нови атаки. Някои от продуктите дават възможност вие самостоятелно да въвеждате образци. Това в значителна степен ви улеснява, но ви натоварва и с нова отговорност ако избраният от вас контрагент се бави с актуализирането на базата данни. Някои от доставчиците извършват тези промени само периодично, например веднъж месечно или дори на тримесечие. Можете да сте сигурни, че в такъв период от време ще има нови атаки, които вие няма да откриете.

2.2.2 Статистически IDS (Statistical-Based IDS)

Вторият основен вид IDS продукти се категоризират като статистически IDS. Вместо да разчитат на образци от предишни атаки, статистическите IDS се опитват да разберат нормалното поведение на мрежата и да класифицират като ненормален всеки трафик, който нарушава това нормално поведение. В продължение на много години статистическите IDS бяха просто лабораторни експерименти. Идеята със сигурност не отговаряше на нуждите на промишлените мрежи. В последно време обаче започна производство на такива статистически IDS, които в известна степен допълват съдържателно претърсващите IDS приложения. Например статистическият продукт научава образеца на пакета за регистриране на потребител и генерира сигнал когато получи пакет за регистрация отличаващ се значително от научения вече образец.

Статистическите IDS страдат от няколко недостатъка. Първият е необходимостта да научат нормалното поведение на мрежата. Тук съществува възможност да сметнат нещо необичайно като нормално. Освен това, за да се намали броя на лъжливите аларми в повечето от този тип IDS се въвежда ниво на чувствителност, което може да се регулира. Ако направим сензорите прекалено чувствителни ще се генерират прекалено много фалшиви алармени сигнали, и това ще доведе до затормозяване на потребителите и администраторите. Намалението на чувствителността пък ще увеличи вероятността за неоткрита злоупотреба с ресурсите на мрежата.

Тясно свързани със статистическите IDS, но обикновено разглеждани като отделна група, са *системите за откриване на аномалии* (*anomaly detection systems* - ADS), понякога наричани още *системи за откриване на аномалии в протоколите (protocol anomaly detection - PAD)*. Тези устройства експлоатират предположението, че има определен краен брой легални начини да функционира даден протокол. Всяко използване на протокола по друг начин се разглежда като подозрително. По същия начин, както статистическите IDS, системите за откриване на аномалии се опитват да идентифицират атаките преди тяхното широко разпространение.

В крайна сметка, в една високо ефективна IDS ще има елементи от всички описани по-горе технологии. Използването на само една технология не може да се справи успешно с голямото разнообразие от Интернет базирани атаки. Но дори и да използваме всичките методи, това не ни гарантира откриването на всяка атака. При избора на IDS трябва да се вземат предвид и някои други фактори.

2.2.3 IDS за хост и IDS за мрежа

В повечето случаи IDS е комбинация от няколко продукта. Частта, която прихваща пакетите в един сегмент на локалната мрежа се нарича *сензор*. Сензорите изпращат данните към IDS устройство, в което е разположена централна база данни. Една база данни е в състояние да наблюдава дейността на множество сензори, обикновено 10 до 20. Тя може да бъде разположена на сървър или отделен хост и включва конзола за управление.

2.2.3.1 IDS за хост (Host-Based IDS)

Първият голям избор, който трябва да направим, и който засяга ефективността на IDS, е да изберем вида на самата IDS – IDS за хост (Host-Based IDS) или IDS за мрежа (Network–Based IDS). Както подсказва името, IDS за хост е система, която се намира на отделен хост в мрежата. Нейната задача е да открива само атаки насочени към този конкретен хост. Предимството на системата е, че можем да имаме голяма степен на доверие в нея, както и информация за всяка атака предприета към дадения хост. Обикновено трафикът към даден хост е подмножество на трафика в цялата мрежа, което ни позволява ефективно да изградим система от разпределени IDS с по-голяма вероятност на откриване на атаките именно поради малкия и специфичен трафик към конкретните хостове.

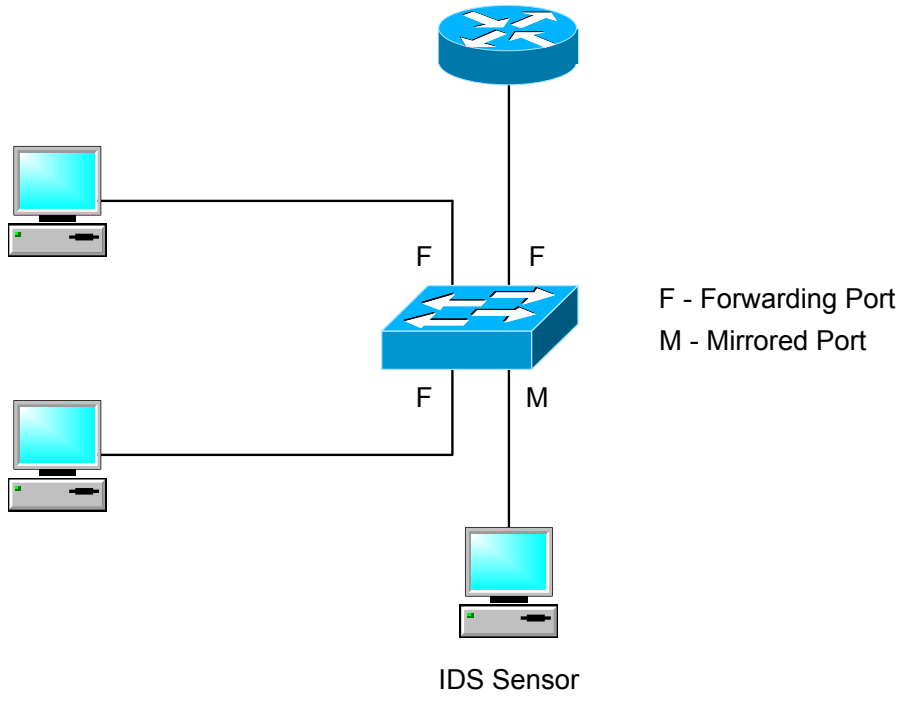
Независимо от това предимство, тези системи имат и редица недостатъци. На първо място, те са зависими от операционната система на хоста. За хетерогенните мрежи това означава множество различни IDS, което води до по-големи административни разходи. Това е особено вярно в случая, когато искаме да покрием с този тип системи всички потребителски работни станции в мрежата. Възникват и проблеми със самото наблюдение на тези разпределени IDS. Ще има ли централно регистриране на събитията, или всеки един от тези хостове трябва периодично да бъде анализиран за своевременно откриване на проникванията? Поради тези недостатъци, IDS за хост обикновено се използват за защита само на особено чувствителни устройства, като например мрежови сървъри.

2.2.3.2 IDS за мрежа (Network-Based IDS)

IDS за мрежа са устройства, които работят в един мрежови сегмент. Функциониращи в т.н. хаотичен (promiscuous) режим, тези устройства записват целия трафик в дадения сегмент. Това им дава предимство спрямо ICS за хост, защото могат от едно място да откриват атаки насочени към много хостове. Освен това една или две ICS за мрежа могат много по-лесно да бъдат наблюдавани, отколкото десетки или стотици IDS за хостове.

Тези системи имат и редица недостатъци. Първият от тях е, че повечето мрежи са комутируеми (switched). За да могат IDS за мрежа да функционират правилно, те трябва да имат достъп до целия мрежови трафик. Това може да се осигури като комутаторите се конфигурират с пренасочване на портовете (port forwarding), известно също като огледално копие на портовете (port mirroring). Пренасочването на портовете е възможност за препращане на трафика между различните портове към специално отделен порт за наблюдение. Не всички комутатори, особено по-евтините, поддържат тази възможност. Освен това, дори да позволяват пренасочване на портовете, те не винаги поддържат възможността да наблюдават едновременно предаваните и приеманите пакети от тези портове.

За да изясним проблемите с огледалните копия на предаваните и приеманите пакети малко ще опростим задачата. На Фиг.2 два от портовете на комутатора са свързани към хостове, а един порт е свързан към маршрутизатора. Имаме и четвърти порт, който сме резервирали като огледален, за наблюдение на трафика.



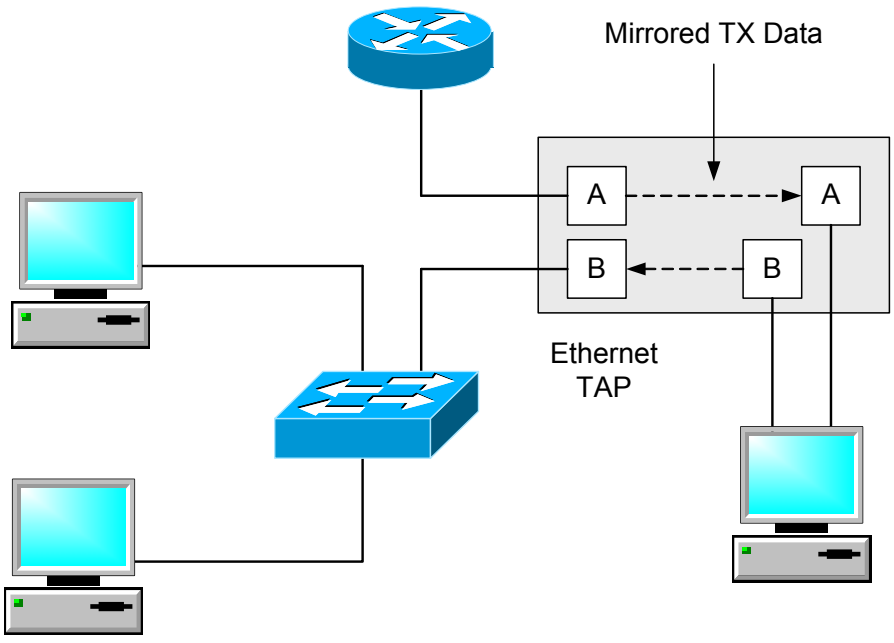
Фиг. 2 Използване на пренасочване на портовете

Решаваме да прихващаме трафика изпращан към маршрутизатора. Как ще направим това зависи от типа на комутатора и от неговите възможности за пренасочване на портовете. Ако комутаторът има възможност да препраща само приемания трафик (от гледна точка на комутатора), то тогава ще наблюдаваме само трафика изпращан от маршрутизатора,

но не и трафика, който той получава от хостовете. В идеалния случай ние искаме да наблюдаваме целия трафик – нещо, които не всички комутатори го могат. Частично това можем да преодолеем, ако пренасочваме трафика на различните VLAN към отделни портове, но тук отново комутаторът трябва да има възможност за такова конфигуриране. Но дори и ако имаме на разположение такъв съвременен комутатор, то възникват проблеми с различията в производителността на IDS за мрежа и на самия комутатор. За да бъдат прихванати всички пакети преминаващи през комутатора, като имаме предвид гъстотата на портовете му, производителността на такава IDS трябва да бъде многократно по-голяма.

Един от начините за заобикаляне на проблемите, които комутаторите ни създават в процеса на откриване на проникванията, е те да бъдат избегнати напълно. Това не означава да изхвърлим комутаторите от шкафовете. Можем да използваме устройство наречено точка за тестване (test access point – TAP), което ни позволява да разклоняваме сигналите на стандартните UTP кабели или оптичните влакна. Такива устройства се използват от известно време и по-точно от момента на масово навлизане на комутаторите като мрежово оборудване. Първоначално те бяха използвани за включване на протоколни анализатори с цел изследване на събитията в определен мрежов сегмент. Понеже IDS е всъщност едно усъвършенстване на протоколния анализатор, същите устройства започнаха да се използват и за включване на IDS.

На фиг.3 е представено включването на една такава точка за тестване. Разклонена е усуканата двойка на UTP кабела, която служи за предаване от маршрутизатора към комутатора. За да може да се наблюдава физическия кабел, IDS устройството използва два мрежови интерфейса. За повече информация вижте например [4].



Фиг.3 Свързване на IDS с TAP

Основното предимство на TAP пред пренасочването на портовете е, че точката за тестване не влияе по никакъв начин на производителността на комутатора. Независимо

от целта за която се използва, тя е невидима за мрежата. Тази невидимост увеличава потенциалната сигурност, тъй като IDS като че ли е отстранена от активния мрежов трафик. Обикновено TAP се поставя между маршрутизатора и комутатора, като по този начин наблюдаваме целия трафик изпращан на маршрутизатора. TAP може да бъде разположен и в други стратегически места в мрежата, като например между сървъра и комутатора. За да се улесни използването на множество точки за тестване, производителите предлагат такива устройства с много гнезда за разклонения и в изпълнение за вграждане в мрежовите шкафове.

Докато точките за тестване лесно се интегрират с комутаторите, то те не са подходящи за някои инсталации. Както беше показано на фиг. 3, една точка за тестване заема два изходни порта. Това е проблем, тъй като нормалният мрежови интерфейсен контролер не е проектиран да приема сигнала, като едновременно с това го препредава, анализира и записва. От тук и изискването IDS станцията да има поне два мрежови интерфейса. Както ще видим по-късно, някои IDS устройства могат да функционират в реактивен режим ресетирайки или блокирайки подозрителни връзки от името на мрежови хостове. За да може да извършва тази си дейност, IDS трябва да знае достатъчно, за да асоциира трафика на връзката с информацията, която записва по двата интерфейса. Не всички IDS имат тази възможност.

И тук, както при всеки технически проблем, има решение. Най-простият начин е да използваме допълнителен комутатор. Двата порта на точката за тестване се свързват към два порта на IDS комутатора, след което конфигурираме в комутатора пренасочване и целия трафик се прехвърля към порт, към който сме присъединили IDS сензор. Този начин на свързване ни позволява да свързваме много точки за тестване и е мащабируем.

Увеличението на скоростта на предаване в мрежата увеличава проблемите с този вид IDS. Производителите могат да твърдят, че техните устройства откриват всички атаки при гигабитови скорости, но трябва да се обърне специално внимание на специализираната литература и да бъдат консултирани лаборатории провеждащи независими изпитания. В лабораторни условия може и да се постигне откриване на нарушения при гигабитови скорости, но в реалния свят горната граница е 300 Mbps. Причините за това широко разминаване се крият в разпалената реклама и в методите на провежданите тестове. В лабораторията имаме ограничен брой наблюдавани връзки и ограничен брой портове, като при това се използват максимални дължини на пакетите. Този начин на тестване позволява всеки продукт да работи в близост до максималните си теоретични възможности.

Реалната производителност на IDS зависи от редица фактори на обкръжаващата среда, включително от броя на активните сесии, размерът на пакетите, а също така и от това, дали пакетите, които обработваме са валидни. Един валиден пакет създава много по-малко работа отколкото пакет, в който се опитваме да открием някакви непоследователни фрагменти от повече от няколко милиона активни връзки.

За да се компенсират намалените възможности за откриване на проникванията при по-високи скорости на мрежата, можем да приложим няколко метода. Всички те по някакъв начин са свързани с разпределение на натоварването на високоскоростните връзки между множество IDS сензори. Трябва да използваме балансиране на мрежовия трафик или трафика на приложенията, като разделим този трафик на няколко ниско скоростни потока и към всеки един от тях да свържем отделен IDS сензор, който да наблюдава

трафика в рамките на своите възможности. При това препоръчително е трафикът да се разделя на потоци към отделни дестинации или за отделни сесии, а не по кръгова схема (round-robin), каквато се използва при балансиране на натоварването в мрежовите устройства. Важно е пакетите от един поток да са свързани смислово, така че IDS да имат възможност да открият свързани пакети като част от една атака.

Друг начин, който е много по-трудно управляем, но е значително по-евтин, е да разположим IDS сензорите по-близо до хостовете и по-далеко от гръбнака на мрежата, където се използват високоскоростни връзки. Макар че все по-често срещаме малки мрежи да използват Gigabit Ethernet връзки, много сегменти на мрежата работят на по-ниски скорости. Като поместим IDS сензорите в области, в които сме принудени да работим на по-малки скорости поради различни причини, можем да изградим добре работещи IDS без да прилагаме скъпи балансирания на приложенията или хардуерни гигабитови IDS.

2.3 Настройки на IDS

Когато първоначално инсталираме едно IDS устройство, то обикновено се нуждае от някакъв вид настройка. Това е така, защото първоначално нормалния трафик на мрежата е в известна степен подозрителен и наподобява някаква атака. Броят на настройките може да бъде значителен, в зависимост от това какви правила се проверяват и от вида на трафика в мрежата. Обемът на работата, свързана с настройката на IDS е толкова голям, че понякога се използва като мощен аргумент при маркетинга на такива продукти. Производителите рекламират продуктите си и претендират, че не се изисква почти никаква настройка и едва ли не след включване на IDS в мрежата, устройството веднага започва да функционира нормално.

Заедно с появата на фалшиви сигнали, свързани с валидните пакети на нормалния трафик, съществува и проблема с невалидните пакетите, които не задействат системата за предупреждение, т.е. пакети които са част от неоткрита атака. Такива пакети създават даже много по-голям проблем на администраторите, понеже, по дефиниция, те не знаят за тяхната поява. Ето защо инсталирането дори на най-великите и мощни IDS продукти кара администраторите да се чувстват неуютно и несигурно.

В процеса на настройката трябва да решим какво да правим с информацията, която IDS произвежда. Една такава система обикновено има възможност да уведомява администраторите за алармени състояния по много различни начини. Използва се изпращане на SMS, електронна поща, или разпечатка на екран. Въпреки различията между отделните производители, IDS информацията или генерира сигнали за аларма, или се записва в регистрационни дневници.

Сигналите за аларма съобщават за събития, на които мрежовият администратор трябва веднага да обърне внимание. Например, една атака, която IDS класифицира като отваряне на вратичка за проникване (backdoor attack) е нещо, за което мрежовият администратор иска да научи незабавно. Сканирането на определен порт пък е нещо, което носи по-малък риск, и може да бъде само регистрирано и оставено за разглеждане на един по-късен етап.

Най-голямата грешка, която правят мрежовите администратори, когато конфигурират една IDS система, е тя да алармира мрежовия администратор всеки път, когато някой сензор

регистрира някоя аномалия. В този случай алармените сигнали стават толкова много, че не смогваме с тяхното анализиране и в крайна сметка изключваме системата напълно. Ето защо, за да можем да използваме системата ефективно, на алармите трябва да зададем различни приоритети.

Най-разпространения начин за приоритизиране на IDS сигналите, е да използваме метод, много подобен на анализа на риска, като задаваме различна тежест на информацията, която прихваща IDS. Всеизвестно е в мрежовите среди, че вашата мрежа може да бъде атакувана или чрез случайно сканиране (цифровия еквивалент на натискане на дръжката на входната врата докато вие се намирате в хола), или чрез насочена „атака" (някой се опитва да разбие вратата и да офейка с каквото набързо отвлече). Понеже повечето IDS позволяват на мрежовия администратор да настройва различни нива на регистриране на сигналите от различни устройства, то има смисъл да се направи задълбочена инвентаризация на мрежовите активи преди всяка настройка на IDS. Ако имаме изградена правилна политика за сигурност, то голяма част от тази работа вече е била извършена по време на анализа на риска.

След инвентаризацията на мрежовите услуги следва да се създаде списък с техния относителен приоритет. Някои системи и приложения са по-важни от останалите. Например системата за планиране на ресурсите (Enterprise Resource Planning – ERP) или системата за връзка с клиентите (Customer Relationship Management – CRM) са с много по-голям приоритет от системата на сървъра за печат. Пощенският сървър може да се разглежда като по-важен от файл сървъра, или обратното. На базата на тази информация, администраторът може да реши да бъде алармиран при предполагаема атака на ERP, а при атака на сървъра за печат да се извърши само регистриране на събитията и те да бъдат анализирани по-късно.

Заедно с приоритетите на ресурсите трябва да обмислим и приоритетите на атаките. Например, ако сте убедени, че вашите ERP сървъри са сравнително защитени срещу DoS атаки (какъвто е случаят при съвременните операционни системи след използването на множество кръпки), то такива атаки могат само да се регистрират. От друга страна, ако в публичното пространство са се появили нови заплахи и вие подозирате, че вашите сървъри не са подходящо защитени за тях, то би трябвало при поява на такъв тип активност в мрежата да бъдете незабавно алармирани.

В мрежите, в които са взети всички необходими мерки, естествено няма 100% гарантирана сигурност, но такива мрежи са сравнително добре защитени и са устойчиви на широко разпространените скриптови атаки. Такъв тип атаки трябва да се разглеждат като атаки с нисък приоритет. Те трябва да бъдат само регистрирани до достигането на определен праг, след което може да се издаде сигнал за аларма. От друга страна, всяка атака, която потенциално дава на нападателя достъп като администратор на системата, следва да се счита за атака с най-висок приоритет.

При определянето на относителния приоритет на алармите трябва да се има предвид и мястото на IDS сензора, който прихваща трафика. Сигналите от сензор, който се намира в сегмента на сървърите естествено са с много по-висок приоритет, отколкото сигналите идващи от сензор, който следи Интернет трафика извън защитната стена.

И накрая, работата по приоритетите на алармените сигнали значително се опростява, ако самата мрежа е в добро състояние от гледна точка на сигурността. А това означава

всички операционни системи и приложения да бъдат осигурени с необходимите последни кръпки, всички процеси да бъдат документирани и потребителите да използват разумно криптиране и автентикация. Това ще позволи голям брой от атаките да бъдат само регистрирани и ще намали времето на администраторите за анализиране на атаки, които и без това вече са се провалили.

Работата по настройката на IDS може да отнеме много време. Системата трябва да бъде научена да игнорира фалшивите сигнали от валидни пакети и само да регистрира алармените сигнали с нисък приоритет. Крайният резултат от тази работа е кратък и сигурен преглед на заплахите, на които е изложена вашата мрежа, и които с малко късмет, са успешно отблъснати.

2.4 Разполагане на IDS в мрежата

Местата, където се поставят IDS в мрежата, зависят от броя на устройствата с които разполагаме. Например, ако имаме само една IDS система, най-разумно е да я поставим между външните маршрутизатори и защитната стена. Такова разположение ни гарантира, че целият трафик ще бъде проверяван за атаки преди да бъде филтриран от защитната стена. Надяваме се IDS да служи като система за ранно предупреждение, която да ни показва пред какви заплахи е изправена защитната стена. Винаги е хубаво да се знае, когато някой се опитва да се промъкне в мрежата.

Основният недостатък на тази конфигурация е, че тя ще генерира голям брой аларми. Понеже нямаме метод, с който да установим със сигурност, кои атаки ще успеят и кои не, броят на атаките увеличава чувствителността на мрежовите администратори и те изразходват много време за анализ на генерираните от IDS доклади.

Някои привеждат различни разумни аргументи да разположите IDS в самата защитна стена. Логиката на тази позиция е, че управлението на IDS тогава ще бъде много по-лесно, тъй като голяма част от подозрителния трафик ще бъде блокиран от защитната стена. Така разположена вътре във вашата мрежа, IDS извършва и важна проверка на правилното конфигуриране и функциониране на самата защитна стена. Това ни позволява да научаваме за проведени срещу мрежата успешни атаки.

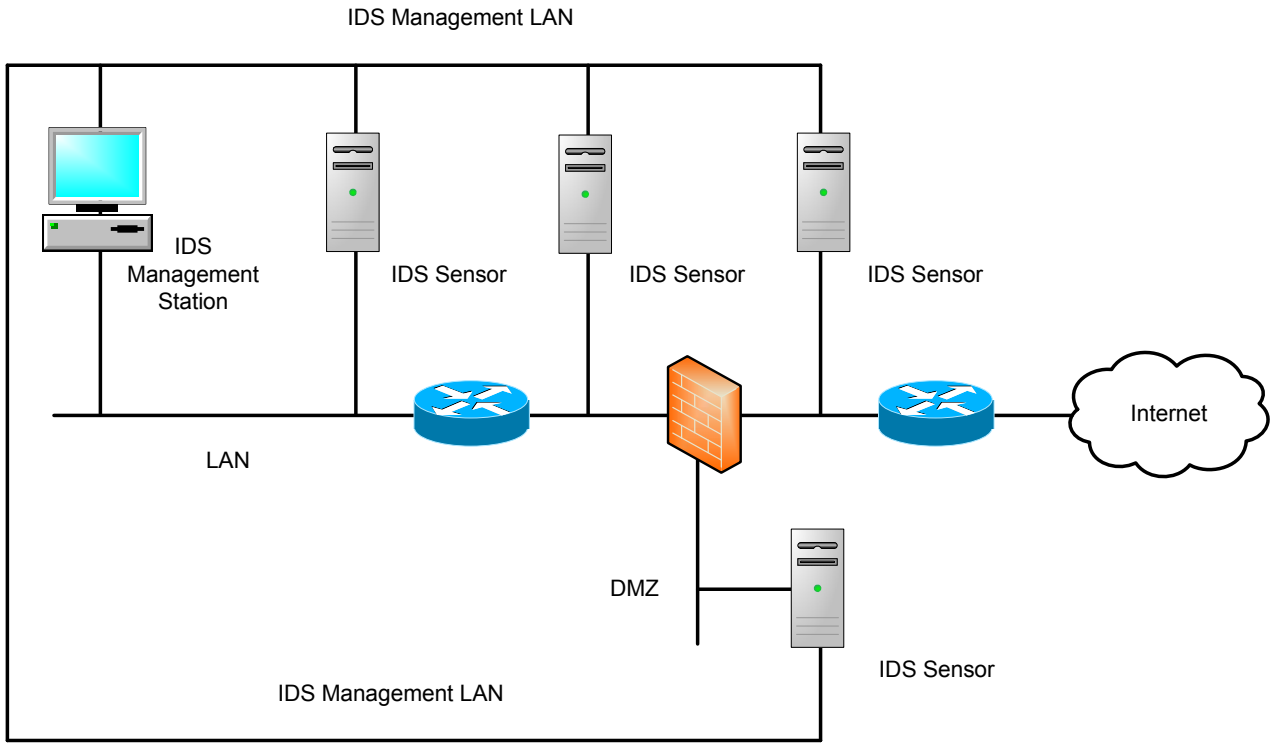
Въпреки че поставянето на самостоятелна IDS вътре в мрежата позволява на администраторите да се концентрират само върху заплахите, които са успели да заобиколят защитната стена, то тези администратори имат вече само ограничен поглед върху това, което се случва извън тяхната мрежа. Те няма да узнават например за атаките, които се провеждат срещу самата защитна стена.

Понеже една самостоятелна станция за управление може да обработва сигналите от много сензори, то често се използва конфигурация, при която се поставят сензори от двете страни на защитната стена. Това ни позволява да сравним информацията си за това на какви атаки е подложена мрежата и доколко защитната стена ни предпазва от тях. Ако ресурсите ни позволяват, IDS могат да бъдат разположени и на други стратегически места в мрежата. Най-честите вторични места на разполагане са демилитаризираната зона (DMZ) и сегментите, където са разположени сървърите. Когато искаме максимално наблюдение на трафика, можем да разположим IDS и в сегментите с работни станции на крайните потребители. Както е при всяко решение засягащо сигурността, броят и

разположението на IDS сензорите следва да отразява приоритетите за сигурност на самата организация.

Във всички случаи IDS следва да се конфигурират в „невидим" режим. Невидим режим означава да не задаваме IP адрес на мрежовия контролер, който наблюдава трафика. Конфигурирането на IDS без IP адрес не позволява на никого извън мрежата да открие устройството и дори да научи за неговото съществуване. По този начин IDS сензорът е предпазен от мрежови сканирания и от атаките, които той се опитва да открие.

Премахването на IP адреса на сензора пречи и на администраторите да наблюдават и управляват процеса (когато използват TCP/IP). Това е от особено значение, когато в една мрежа са разположени няколко сензора и една централна станция събира информацията от тях. За да защитим IDS сензорите, и едновременно с това да извършваме тяхното дистанционно управление, най разумно е да имаме два мрежови интерфейса. Единият интерфейс се използва като сензор и е конфигуриран без IP адрес. Вторият интерфейс обикновено се свързва в отделна локална мрежа, чиято единствена цел е събирането на информация и управлението на различните IDS устройства. Пример на такава конфигурация с четири IDS сензора е показан на Фиг. 4.



Фиг.4 Свързване в отделна локална мрежа на IDS сензорите и станцията за управление

2.5. Реактивни IDS

IDS обикновено е пасивно устройство в мрежата. То тихо прослушва трафика и генерира изход, който се анализира от системния администратор. Устройството има големи възможности за алармиране на администратора при появата на значителни заплахи. Като имаме предвид обаче времето на отговор на компютрите сравнено с това на хората, човекът реално би могъл да реагира на атака тогава, когато тя вече е завършила. Най-

доброто нещо което администраторът може да направи е да анализира дневника и да определи дали атаката е била успешна.

С течение на времето системните администратори започват да осъзнават, че в някои случаи IDS системата може да отговори на атаките вместо тях. Това е различно от защитната стена, където най-общо имаме статична конфигурация. Там пакетите се филтрират на базата на адреси, протоколи и портове. Ако желаете да позволите достъп на отдалечен хост до уеб сървър, трябва да позволите трафик през защитната стена с местоназначение порт 80. За да се защитим от атаки срещу уеб сървъра, ние можем да забраним трафика към порт 80, но тогава ще блокираме целия законен трафик към сървъра. Разбира се имаме възможност да блокираме трафика на основата на IP адреса на източника, но това може да стани само, ако ние вече знаем, че някой е използвал определен адрес за нападение , т.е. вече е имало успешна атака.

Много ще е хубаво, ако IDS сама може да организира защитата срещу атаки, които току що е открила. Това би премахнало бавната човешка реакция от затворения кръг. Ако някой се опита да атакува нашият хипотетичен уеб сървър като използва добре познатото прекосяване на директории, IDS би могла да изпрати към източника на атаката пакет за преустановяване на TCP сесията от името на уеб сървъра, след което да преконфигурира защитната стена така, че трафикът от този адрес да бъде блокиран. Нападателят ще бъде спрян от IDS, а останалите потребители могат да продължат да използват мрежата. Това звучи твърде хубаво, за да бъде истина.

Идеята за „реактивна" IDS, макар и не нова, не среща широко разпространение. От първостепенно значение е това, че пакети с подменени IP адреси на източника (spoofed IP packets) могат да бъдат използвани за провеждане на атаки от типа отказ на услуга (DoS). Ако например искам да попреча да използвате определен мрежов ресурс, мога просто за създам пакет, който да изглежда като че ли идва от ваш компютър и е начало на атака. По този начин вашият достъп до мрежовите ресурси ще бъде ограничен вследствие на мои действия. Представете си тази ситуация в много по-голям мащаб, с десетки хиляди пакети и ще разберете, че възможността от злоупотреба е голяма.

Независимо от това, идеята за реактивни IDS е твърде добра, за да умре от такива „малки" технически пречки. Някои от предложените възможности за реактивни IDS включват, както беше споменато по-горе, възможността активно да възстановяват TCP връзки, като сами изпращат пакети с подменени IP адреси и динамично преконфигурират правилата на защитната стена, в отговор на заплаха, като това става в почти реално време. Други възможности включват спиране на изпълнението на процес в хост, заключване на потребителски акаунти, и изпращане на SNMP съобщения от типа "trap" към устройствата.

2.6 Интегриране на защитната стена с IDS устройство

Като имаме предвид взаимно допълващите се роли, които играят защитната стена и IDS, не трябва да се изненадваме, че производителите са създали устройства „всичко в едно". Този тип устройства със сигурност улесняват интеграцията между реактивните IDS приложения и приложенията на защитната стена, тъй като и двете устройства използват един и същ хардуер.

Защитната стена може да бъде интегрирана и с VPN шлюз. Изобщо при интегрирането на няколко различни по своите функции устройства за сигурност в едно устройство, винаги получаваме определени предимства и недостатъци. От една страна, когато всички защитни функции се намират в едно устройство, сигурността на мрежата може по-лесно да бъде тествана, наблюдавана, конфигурирана и управлявана. Тъй като основна заплаха за информационната сигурност е твърде сложната конфигурация на мрежовите услуги, то очевидно е, че колкото е по-голяма е интеграцията на защитната стена с IDS, толкова по-лесно и безпроблемно те ще бъдат конфигурирани.

От друга страна, уповаването на само едно устройство за мрежова сигурност е рисковано предложение. IDS служи и за проверка на конфигурацията на защитната стена, а системата за регистриране служи за проверка на дейността на мрежата след определени събития. Ако всички тези системи бъдат поставени в едно единствено устройство, достатъчна е само една успешна атака към това устройство, и това да се окаже опустошително за цялата мрежа. Не само че вашата защитна стена ще бъде компрометирана, което само по себе си е сериозен инцидент, но вие ще загубите и способността да разберете за това.

Макар че разделянето на услугите по сигурността между различни устройства увеличава усилията за управление на системите , то също така и дава възможност за гарантиране на целостта и работоспособността на различните системи – дори и след като мрежата е била изложена на риск.

Няма еднозначен отговор на въпроса дали да използвате устройство, в което са интегрирани двете функции. Решението трябва да вземете вие, и то само след като сте наясно с последиците от него и как то ще повлияе върху вашата политика за сигурност.

2.7 Други видове IDS

„Традиционната" концепция на използване на IDS не е единственото оръжие в арсенала за мрежова защита. Ако вашата политика по сигурността го изисква, има и други мрежови елементи, които могат да бъдат включени като част от цялостната IDS стратегия.

Системите за откриване на нарушители са полезни, тъй като те предупреждават за съмнителна мрежова активност. Проблем обаче е да определим, дали откритата атака е била успешна. Най-добре е дейността по регистрирането на достъпа да се извършва на отделен хост, който от своя страна да бъде сигурен. От гледна точка на сигурността обаче, почти никога не знаем със сигурност дали вашата система, вашата IDS или системата за регистриране е сигурна. IDS системите за мрежа или хост само откриват атаки и други аномалии на мрежово поведение. Те обаче не дават информация за това, дали са направени легитимни промени в хостовете по мрежата и дали някой е получил физически достъп до хоста чрез локален терминал или флаш памет. Повечето IDS за мрежа не са в състояние да разберат за такива злоупотреби или промени. Ако искаме да знаем за тези събития, задължително е да използваме проверка на целостта на файла (file integrity checker).

Проверката на целостта на файла е софтуерна програма, която изчислява MD5 хеш суми на всички програми на даден хост. За всеки файл се изчислява индивидуална хеш сума. Тази сума се записва. Целта на програмата за проверка на целостта на файла е да позволи на мрежовия администратор да следи измененията в хиляди файлове и

изпълними програми, които се намират на даден хост. Периодично, или когато мрежовият администратор подозира за някакъв вид компрометиране на мрежата, се стартира тази програма. Ако новата стойност на MD5 хеша е различна от старата стойност, то е ясно, че са настъпили някакви промени във файла.

В някои случаи промените във файла са очаквани. Такива са файловете, които се пазят в кеш или временни директории. Други файлове се променят при нормално използване, например файловете на база данни или файловете в потребителските директории. Изпълнимите файлове обаче се променят рядко, ако изобщо трябва да се променят. Системният администратор е този, който трябва да определи кои промени във файловете са допустими и легитимни и кои не. Всички програми за проверка на целостта на файл, които се намират в търговската мрежа, позволяват конфигуриране, така че мрежовият администратор да не подлага на проверка някои често използвани файлове.

Програмата за проверка на целостта на файл не ви позволява да определите каква промяна е настъпила. Тя само ще потвърди, че файлът е променен. Успехът на тази програма се дължи на интегритета на MD5 хеша, поради което не е препоръчително стойностите на хеша да се пазят на хоста, който се опитвате да защитите. Ако в този хост вече има вирус от типа „троянски кон”, то той може да модифицира хеш стойностите по такъв начин, че те да отговарят на направените промени. В идеалния случай хеш стойностите могат да бъдат записани на CD и да се съхраняват на сигурно място до следващата проверка.

Програмите за проверка на целостта на файловете са от съществено значение при определянето дали са правени промени в даден хост. Мрежовите администратори могат да се опитат ръчно да наблюдават тези хостове, но това се оказва непосилна и в крайна сметка безполезна задача. Типичните UNIX системи имат около 60 000 файла и дори да отстраним всички ненужни файлове, то пак ще останат над 15 000 файла. Неприемливо е използването на времето на администратора за търсене на промени в самите файлове или във времената за достъп до тях. Много програми от типа „троянски кон” могат да прикриват промените в програмите, а понякога да скриват и цели приложения от типа „задна вратичка”, при претърсване на директориите и преглед на списъка от изпълняващите се процеси. В този случай дори и най-проницателните и способни мрежови администратори няма да могат да определят дали техните системи са били компрометирани просто като проверяват сами файловете.

Докато програмите за проверка на целостта на файловете може да се разглеждат като необходимост в хост машините, то има и друг инструмент на мрежовата сигурност, който е информативен, но някои го смятат за изключително важен.

Инструментите, които нападателите използват срещу мрежовите системи, са в непрекъснато развитие. Старите инструменти, които се възползват от миналогодишни уязвимости, вече не са актуални, тъй като са направени системни кръпки. Разработват се нови инструменти, които да се възползват от новооткрити уязвимости. За професионалистите по мрежова сигурност, проблемът е да се определи какви са новите атаки преди те да бъдат използвани срещу мрежата и да причинят вреди или да компрометират поверителна информация. Един нов подход към решаването на този проблем е да създадем отделна система, чиято единствена цел е да бъде атакувана и разбита. Това е известно като използване на капан наречен “honeypot”.

Honeypot, както подсказва превода на името му (гърне с мед), е привлекателно изглеждащ сървър в мрежата, който е разположен там само за да примамим някой да разбие неговата защита. Отделно от него е разположена една IP-невидима система, която действа като мрежов анализатор и която записва всички пакети към и от този сървър. След разбиването на сървъра, пакетите се изследват, за да определим метода, който е използван за компрометиране на системата. Един път разбрали същността на метода, вече не е трудно всички реално действащи сървъри в мрежата да бъдат защитени срещу тази нова заплаха.

Honeypot е много полезен срещу често срещаните скриптови атаки в Интернет. Използвайки прекомпилирани заготовки, много хакери с ограничени технически умения, са в състояние да нанесат големи щети в мрежите. При този клас атаки има голяма вероятност за компрометиране на всеки достъпен сървър. Това не означава, че honeypot не може да се използва за записване на действията на по-опитни хакери. Просто групата на високо квалифицираните хакери е по-проницателна при проучване на целите си и се стреми да завладее хостове, които да бъдат използвани в последствие за постигане на крайните цели, а не разбиване на всяко нещо, което изглежда интересно и с което могат да се справят.

Има honeypot продукти, които могат да емулират няколко операционни системи. Ако ви трябва например сървър, който емулира Apache Web Server с Red Hat Linux 6.0, то трябва само да изберете това като опция при конфигурирането. Ако искате да го промените на IIS сървър, избирате друга опция. Понеже honeypot е преди всичко средство за обучение, то най-добре е да използвате реален сървърен софтуер. Едновременно с обучението ви по често срещани атаки в Интернет, вие ще увеличавате и своите умения за защита на сървърите срещу такива атаки. Най-простият honeypot е просто един сървър, който е създаден и не предоставя никакви реални услуги. Тъй като сървърът не обслужва мрежови ресурси, всеки достъп да него ще изглажда подозрителен. Акаунтът на администратора може да бъде променен от “Administrator” на някакъв друг, и всеки опит за достъп до сървъра като администратор автоматично ще генерира предупреждение.

За да увеличим максимално неговата ефективност, honeypot трябва да бъде конфигуриран с известна степен на сигурност. Това преследва две цели. Първата е, че нищо няма да научим от атаки, за които знаем всичко. Има достатъчно документация как да защитим мрежата си в значителна степен. Тази документация трябва да бъде използвана, а не отново да я преоткриваме. Ако сте положили достатъчно усилия за създаването на honeypot, то вие ще искате да извлечете и максимална полза от него. Втората причина е, че напълно незащитен сървър ще изглежда подозрително. Въпреки че броят на незащитените сървъри в Интернет все още е отчайващо голям, хакерите знаят за honeypot, и могат да бъдат подозрителни от съществуването на голяма мрежа с намиращ се в нея напълно незащитен сървър.

Honeypot може да бъде разположен на различни места в мрежата, в зависимост от целите на сървъра. Повечето организации го поставят извън обичайната си защитна стена. Това позволява лесен достъп до сървъра, като едновременно с това не подлага на риск истинската мрежа. Не е рядко явление обаче, да поставите honeypot във вътрешната мрежа, за да заловите служители, които могат да бъдат по-любознателни, отколкото корпоративната политика за сигурност им позволява.

И при двете местоположения трябва да имаме включен мрежов анализатор или даже IDS, който да следи целия трафик към honeypot. Както при нормалното разполагане на IDS, интерфейсът на сензора не трябва да бъде конфигуриран с IP адрес. Устройството ще подслушва трафика, но ще остава невидимо от гледна точка на мрежовия слой. Разпечатването на дневниците на хартиен носител или на CD може да достави много полезна информация за действията на атакуващия хакер.

Използването на механизъм за сигурност като honeypot може да се окаже понякога доста сложно от юридическа гледна точка. Някои организации създават honeypot като капан за примамване, заклещване и последващо преследване на лица и групи, опитващи се да компрометират техните сървъри. Границата между примамването (enticement) и заклещването (entrapment) може да бъде доста тънка. Примамването е законно, но със заклещването не е така. Простото поставяне на атрактивен сървър с няколко уязвимости в мрежата е пример за примамване. От атакуващите зависи дали ще открият примамката и ще се възползват от ситуацията. Заклещването от друга страна, би било действие на „издърпване" на потребителя към сървъра, за да се регистрира неговата дейност. Например рекламирането на пиратски софтуер в една дискусионна група с последващ запис на действията на всички, които са влезли да търсят такива файлове, ще се разглежда като заклещване.

Активното привличане на внимание в Интернет може да доведе и до други неприятни последствия. Въпреки че се надявате да заловите и преследвате атакуващите лица, в действителност може да откриете, че тези лица са извън вашата юрисдикция и са недосегаеми за правоприлагащите органи според законите на тяхната страна. Като резултат от многото усилия за проследяване на нападателите, можете да откриете група гневни хора в другия край на света, върху която администраторът не може да упражни никакво въздействие. Освен това администраторите могат да открият, че са привлекли много голямо внимание и са подложени на допълнителни хакерски атаки към производствените мощности на корпорацията и атаки от типа отказ на услуга в мрежата като цяло.

Honeypot е интересно устройство за обучение по мрежови атаки и защита на мрежови ресурси; то със сигурност не е най-подходящото средство за залавяне на нападатели. С негова помощ можем да намерим необходимата информация за начина на атаката, но използването на нормалните процедури за сигурност ще ни снабдят с тази информация по един или друг начин.

Много информация за конкретните устройства, които се произвеждат, за техните възможности и конфигуриране, можете да намерите например в [5] и [6].

3. Литература

[1] Стоилов, Е: Уязвимост на системите при свързване на корпоративните мрежи с мрежите за управление на технологични процеси, Автоматика и информатика, № 3, 2010 .

[2] Стоилов, Е.: Сигурност в системите за управление на технологични процеси, Технически доклад, 2010, http://eprints.nbu.bg/466/

[3] Проект Honeynet, http://project.honeynet.org

[4] OPTOCON SFT-TAP, Test Access Point Splitter,
http://www.methode.com/static/cms_workspace/pdf/Data/CPL_02-07_EN-SFT-TAP.PDF

[5] Cisco Intrusion Detection Systems,
http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html

[6] Cisco Intrusion Prevention Systems,
http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html