Срок за предаване
на дипломната работа: 1.12.2010.....
Ръководител:.....

Съдържание

Увод

Развитието и глобализацията на информационните технологии доведе до повишаване риска от достъп на неоторизирани лица до данни и ресурси на корпоративните компютърни мрежи. Това естествено наложи разработването на специфични устройства и софтуер за защита на информацията в съвременните комуникационни и информационни системи.

За да съществува и да се развива всяка структура по света (правителствена, бизнес организация, неправителствена организация) се нуждае от определено ниво на сигурност и защита. Сред законите на всяка страна съществуват разпоредби за търговската и държавна тайна както и правата на интелектуална собственост, а официалната власт използва най-различни практики за наблюдение на комуникациите между гражданите (не само на техните страни), за да предотвратят престъпна или нежелана политическа дейност. Съдебните системи в повечето демократични държави могат да издават разпореждания по молба на правителствените агенции за прилагане на специални разузнавателни средства (СРС).

Значимостта на проблема за защита на информацията в дадена структура се дължи на следните факти:

- Променена е спецификата и значимостта на информационната среда, която вече се разглежда като обобщена (интегрирана) и частна и една специфична предметна област е информационната сигурност;
- Проблемно в наши дни се оказва огромното увеличение на обема информация, до която министерства, престъпници,

конкуриращи се организации или просто любопитни хора се опитват да достигнат;

- Информацията представлява повече от 50% както от бизнес дейностите така и от личните. Поради увеличения обем на сведенията и тяхното нараснало значение, потенциалното проникване от неоторизирани лица в базите данни (БД) или вътрешни организационни комуникации може да има такива последствия, които да доведат до ефект преоформящ цялостно дадената структура.

Макар, че това са основните причини, които карат индивидите и институциите да обръщат особено внимание на защитата на информацията, не бива да забравяме и така необходимия **институционален престиж**.

Нито една, уважаваща себе си структура или индивид, не може да позволи накърняване на реномето си чрез пропуски в защитната система за опазване на необходимата и информация и комуникации.

Спецификата и значимостта на информационната среда, е задълбочено изследвана и анализирана в книгите на проф. С. Денчев „Информационна среда за трансфер на технологии" и съавторската с проф. Д. Христозов „Несигурност, сложност и информация: анализ и развитие на несигурна информационна среда". В началото на този по същество монографичен труд е направено разграничаване между **обобщена** (интегрирана) и **частна** информационна среда. Последната представлява множество от три функционално свързани компонента: **информационни фондове, информационни технологии и човешки фактор**, проявяващ се в интеракциите между субектите и оборудването (Денчев, С., 2003). В зависимост от характера на информационните процеси, за които тя се отнася информационната среда би трябвало да има съответна специфика. Една специфична предметна област на информационната среда е **информационната сигурност**.

Проблемите на информационната сигурност и защитата на информацията в компютърните системи трябва да бъдат обмислени още в процеса на проектиране на информационата среда. Когато една „информационна среда" вече е „създадена" и се експлоатира, е много трудно към нея да се добавя като „кръпка" цялостна система за информационна сигурност. От една страна, самата защита няма да е достатъчно ефикасна, а от друга процесът на добавянето във всички случаи е неоправдано трудоемък.

Всичко това е довело до вече съществуващ развит пазар, разрешаващ въпросите на защита в определени граници. Ключовият момент е, че прилаганите системи за сигурност трябва да осигряват равновесие между пълната неприкосновеност за определени национални структури и възможността за наблюдение на информационните транзакции на останалите организации и индивиди от една страна, а от друга до гарантиране на неприкосновеноста до необходимото ниво за поддържане на виталността на *непривилегированите* структури. Решаването на тези въпроси има както технически така и морален аспект.

Целта на настоящата разработка е да се запознае заинтересованата аудитория с предпоставките при взимане на решение за определяне на външната и вътрешната защита на информацията в корпоративната „INTRANET".

Основните задачи за нейното постигане са:

- преглеждане на литература и публикации от областта на информационните технологии, информационната сигурност и защита на информацията в автоматизираните системи и/или мрежи;
- участие в I и II семинар по проблемите на информационната сигурност на Сага Технолъжи и ДАИТС;

- изясняване на технологичната база на Intranet, нейните основни черти и решавани задачи в нея;
- изграждане на концепция за „политика за сигурност” в корпоративната „Intranet”;
- Решения за „защита от ПЕМИ”;
- Анализиране на системата за управление и защита
- Възможности за използване на „биометрична защита”;
- Решения за „криптиране и кодиране на информацията”.

Основен обект на изследване в дипломната работа е корпоративната „Intranet”.

Предмет на изследването е организацията, управлението и защитата на информацията в нея.

От основно значение е определяне и въвеждане на добре осмислена и балансирана политика за сигурност, която да бъде рамкирана и изграждана (по възможност) от самото начало на съществуване на конкретната организация.

ГЛАВА ПЪРВА

Корпоративна Интранет и политика за сигурност

1.1. Корпоративна Интранет - същност

Технологията Интранет представлява използване на Интернет технологията и TCP/IP-мрежите за изграждане на мрежова и информационна инфраструктура на корпоративни или кампусни (университетски) мрежи. Тя е „заела" от Интернет всички важни протоколи и приложения. Интранет по същество се явява ефективно използване на технологиите на глобалната мрежа Интернет за решаване на корпоративни задачи и средство за WEB интеграция на корпоративни (затворени) и отворени мрежи Интернет.

1.1.1. Технологична база на Интранет

- Използване на протоколния стек TCP/IP и по-специално върху него HTTP (за създаване на приложения WWW);
- Виртуални локални мрежи, използващи протокола VLAN и LANE, частни мрежи и виртуални частни мрежи (VPN) върху IP;
- Технологичният клиент/сървър и по-нови компонентни технологии и олекотени клиенти.

1.1.2. Основни черти на Интранет

- Използване на технологията WWW за обмен на информация вътре в корпоративната мрежа (достъп/ преглеждане и публикуване) – HTML/WWW Publishing – XML;
- Осигуряване на безопасен достъп до ресурсите на мрежата отвън-навътре, преобразуване и транслиране на адресното пространство на корпоративната мрежа – Firewall, Proxy, Cache;
- Единна система за електронна поща, използваща стандарта MIME, PGR/PEM, X400и обединяваща различни пощенски системи (Ms Exchange, Eudora, Netscape Mail);
- Единна система на директории за търсене на потребителите на мрежата, организации и подделения – Yellow Page, X.500, Whois
- Единна навигационна и търсеща система по ресурсите на мрежата =- WAIS, Alta Vista, CWIS;
- Поддръжка на бизнес приложения чрез Интернет (осигуряване на безопасна търговия през Интернет, създаване на „тунели" за свързване на подделенията на корпурацията чрез Интернет);
- Средства за поддържане на корпоративна работа на групи потребители (посредством WWW, електронни конференции, видеоконференции, списък с адреси);
- Мобилност на потребители и приложения – видове мобилност в разпределените системи – Oracle VAP.

1.1.3. Основни задачи решавани в Интранет

- Единна стандартна технология и технологична база, позволяваща обединяването на множество приложения на основата на технологията клиент/сървър – хоризонтална съвместимост – други варианти и задачи на интеграцията, дори и в условията на различни технологии и бази;

- Възможност за развиване и усъвършенстване на отделни компоненти на системата и еволюционното и развитие – вертикална съвместимост;
- Мобилност на приложенията и потребителите;
- Разделяне и съвместно използване на ресурсите на мрежата;
- Интеграция на дейностите и ресурсите;
- Предпоставки за развитие на технологията Интранет и нейни приложения;
- Технологията Интранет е предоставила ефективни възможности за решаване на корпоративни задачи и е решила проблема с принудителното обединяване. Корпоративните мрежи и отворения Интернет, също така предостави и възможности за комерсиалното му използване – за маркетинга, търговията, интеграцията и търсенето на информация;
- Развитието на Интернет в глобален мащаб и ръстът и броя на потребителите;
- Създаването на WWW като универсално съвременно средство за достъп до ресурсите на Интернет, по качество на представяне на информацията и възможности за визуализация сравнимо с тележизията и непосредствена работа;
- Създаване и развитие на технологията на виртуалните мрежи, ATM, клиент/сървър, VPM;
- Решаването на задачата за осигуряване на безопасността за предаването на информация в разпределена (нецентрализирана) инфраструктура, за разлика от преди разработената концепция за безопасност DOT/Internet, използваща централизирана инфрастриктура за осигуряване на безопасност.

1.1.4. Интранет и миграция

- Интернет технологиите в Интранет се явяват резултат и от продължителната синергия на две концепции за развитие на Интернет;
- Университетска, предоставяща безплатно некомерсиални ресурси на индивиди за създаване на свободно разпространявани обществено достъпни продукти;
- Корпоративни или комерсиални, използващи принципа на комерсиализиране на покупни ресурси за създаване на корпоративни продукти, намиращи се в последствие в корпоративна (частна) собственост.

1.2. Политика за сигурност

Проблемът за защитата на класифицираната информация в корпоративната INTRANET е нов. Въпреки широкото му обсъждане в обществото, все още е трудно да се намери отговор на следните въпроси:

- Как да се създаде организация за защита на информацията в конкретно учреждение или предприятие?
- Как да се изгради надеждна и сигурна система?

Законът не дава отговор на тези въпроси. Цел на информационната сигурност[1] е постигането на: поверителност, цялостност, достъпност и проверка за автентичност.

Защитата на класифицираната информация се изразява в комплекс от мерки в областта на физическата, документалната, персоналната и компютърната сигурност. Не всички мерки са технически. В тези области е възможно да се прилагат различни мерки, които са описани в настоящата работа.

[1] По подробно определението е дадено в Петров, Р., Защита на информацията в компютрите и мрежите, Издателство „Корени", С., 2002.

1.2.1. Управленски мерки

Те означават да се разработи политика, програми за сигурност, анализ и управление на риска.

Под **политика за сигурност** може да се разбира съвкупност от управленски решения по отношение защитата на класифицираната информация и присъединените към нея ресурси. От практическа гледна точка политиката за сигурност може да се раздели на три нива.

Към **първото ниво** са решенията, които имат отношение към цялата организация. Те се вземат от ръководството на организацията и са с по-общ характер, като например: решение да се проектира или преразгледа комплексна програма за защита на информацията; формулиране на целите, които преследва организацията в областта на защитата на класифицираната информация; осигуряване на база за спазване на законите и наредбите; систематизиране на управленските решения по въпросите за реализация на програмите за защита, които са валидни за цялата организация. Към това ниво на управление се отнасят защитата на ресурсите и координацията при използването на тези ресурси, обособяването на специален персонал за защита на критично важни системи, поддържането на контакти с други организации и пр. Политиката за сигурност от това ниво има връзка с три аспекта: п*ърво*, организационната единица[2] е длъжна да спазва съществуващите закони; *второ*, трябва да контролира действията на лицата, които отговарят за изработване на програмите за сигурност; и *трето,* да се осигури определена степен на отговорност на персонала.

Към **средното ниво** се включват отделни аспекти на защитата на информацията. Като пример за това е достъпът до интернет (как да се съчетае правото да получаваш информация със защитата от външни заплахи), използването от потребителите на нелицензирани програми и

[2] Така се определят в закона организациите и фирмите, работещи с класифицирана информация.

т.н. Политиката за сигурност на това ниво има отношение към следните теми:

- Описание на аспекта, т.е. описанието на заданието и конкретните изисквания към мрежата - с каква информация ще се работи, с какви ресурси се разполага, на какви изисквания за защита трябва да отговори системата и т.н.
- Обхват и ниво на сигурността. Например за АИС и/или мрежи на важно държавно учреждение (МВР, МО и т.н.) може би трябва по-висока степен на защита, отколкото на една малка фирма;
- Сфера на използване, т.е. къде, кога, как, по отношение на кого и какво се приема дадената политика за сигурност;
- Позиция на организацията по дадения аспект, т.е. целите на организацията по отношение на защитата на класифицираната информация. Най-добрите политики за сигурност на данните използват превантивния подход. Чрез предотвратяване на възможността за неоторизиран достъп данните ще останат защитени;
- Права и задължения на лицата, отговарящи за провеждането на политиката за сигурност. Тези права и задължения се определят със Закона за защита на класифицирана информация (ЗЗКИ) и Наредбата[3], както и с вътрешни нормативни правила. Политиките определят насоките и правилата, които могат да бъдат от полза на администраторите и потребителите при възникване на непредвидени ситуации в мрежата. *Например,* ако трябва да се проверяват дискети от друг компютър, е необходимо да се опишат процедурите за проверка. Ако не трябва да се използват нелицензирани програми, трябва да се знае кой отговаря за изпълнението на това правило и т.н. Най-общо, групите хора, които имат отношение към сигурността на информацията в една система или мрежа са: ръководителите,

[3] Наредба за задължителните общи условия за сигурност на автоматизираните информационни системи/мрежи, в които се създава, обработва, съхранява и пренася класифицирана информация.

системните инженери, системните администратори, системните организатори и потребителите;

- Законосъобразност. Политиката за сигурност трябва да съдържа общо описание на забранените действия и наказанията за тях. Случаите на нарушения от страна на персонала трябва да се разглеждат от ръководството и да се предприемат наказателни мерки, включително и уволнение;
- При определяне на политиката за сигурност трябва да се знае всеки служител от кого може да получи разяснение, помощ и допълнителна информация;

Политиката за сигурност на **най-ниското ниво** се отнася до конкретното програмно осигуряване. За разлика от предишните две нива тя трябва да бъде доста по-детайлна. Въпросите, на които трябва да се отговори при определяне на политиката за сигурност за това ниво, са например:

- При какви условия могат да се четат и модифицират данните в АИС?
- Кой има право на достъп до обектите, поддържащи програмното осигуряване?

Формулирането на целите на политиката на най-ниското ниво също се основава на съображенията за поверителност, достъпност и цялостност, но тези цели трябва да бъдат по-конкретни.

От целите произтичат правила за защита на информацията, описващи кой, какво и при какви условия може да върши. Колкото са по-детайлни правилата, толкова по-лесно е да се изпълняват програмно-техническите изисквания. От друга страна, много строгите правила може да пречат на работата на потребителите. Затова ръководството ще трябва да намери разумен компромис, при който за приемлива цена може да се осигури приемливо ниво на защита, без да се ограничават служителите.

След като се определи политиката за сигурност на една система, може да се пристъпи към изготвяне на **програма за сигурност**[4] и към нейното реализиране. Програмата може да се структурира също на отделни нива, съответстващи на структурата на самата организация. В най-честите случаи са достатъчни две нива: централно и изпълнителско.

Програмата на централно ниво се отнася за цялата организация и може да се ръководи от лицето, отговарящо за сигурността на информацията в АИС и/или мрежите, като главните й цели са: оценка на рисковете и заплахите; избор на ефективни средства за защита; координация на дейностите на различни отдели и служители при защитата на информацията; стратегическо планиране; контрол на дейностите в областта на защитата на класифицираната информация.

Целта на програмата на изпълнителско ниво е да осигури надеждна и икономична защита. На това ниво се решава какви механизми на защита могат да се използват, закупуването и установяването на технически средства и т.н. За изпълнението на действията по програмата трябва да отговаря администраторът на мрежата.

Програмата за сигурност не бива да се превръща в набор от технически средства, построени в система, защото така ще загуби своята независимост и авторитет и като следствие висшето ръководство ще забрави за нея.

1.2.2. Анализ и управление на риска

Дейностите на една организация, работеща с класифицирана информация, са изложени на много рискове, още повече когато тази информация се разпространява по АИС и/или мрежи.

[4] По подробно този елемент е развит в учебника на Павлов, П., Актуални информационни технологии в отбраната и сигурността, УИ „Стопанство", 2001.

Започва се с избор на анализируемия обект. За неголеми организации може да се разглежда цялата информационна инфраструктура, но за крупни организации това може да се окаже необосновано скъпо и бавно. В тези случаи ще трябва да се анализират най-важните възли от мрежата. При анализа на риска са уязвими всички елементи от информационната система - от мрежовия кабел, който може да се прекъсне, до базата от данни, която може да бъде разрушена от неумелите действия на администратора. Много е важно да се избере разумна методология за оценка на риска**.** Целта на оценката е да получи отговор на два въпроса: Приемливи ли са съществуващите рискове и ако не, какви защитни средства е икономически изгодно да използваме? Това означава, че оценката е количествена. Управлението на риска е типична оптимизационна задача и съществуват достатъчно програмни средства, с които да се реши. Анализируеми обекти са: класифицираната информация, компонентите на информационната система, програмните ресурси, поддържащата инфраструктура, персоналът. Следва да се класифицират данните по нивото на сигурност[5], да се определят местата за съхранение и обработка, начините за достъп до тях. Важно е да се систематизират обектите, за да може да се направи оценка за последствията от нарушаване на защитата на информацията.

Рискът се появява там, където има заплаха. Като правило наличието на една или друга заплаха е следствие на слабости в защитата на АИС и/или мрежите, което се обяснява с отсъствието на някои програмно-технически средства за сигурност или в недостатъци в реализиращите ги защитни механизми. При определянето на заплахите за класифицираната информация в АИС и/или мрежите също се прави идентификация. Анализируемите видове заплахи следва да се избират на базата на здравия разум (като оставим настрана например заплахата от

[5] По подробно този въпрос е развит в гл. 4 на учебника: Павлов, Г., Информационни технологии в отбраната и сигурността, УИ „Стопанство", 2003. В ЗЗКИ се определят три нива: „строго секретно", „секретно", „поверително" и „за служебно ползване".