ЎЗБЕКИСТОН РЕСПУБЛИКАСИ

ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

НАМАНГАН МУҲАНДИСЛИК-ПЕДАГОГИКА ИНСТИТУТИ

Алишер Анваров

МАЪЛУМОТЛАРНИ МУҲОФАЗА ҚИЛИШ

ФАНИДАН

МАЪРУЗАЛАР КУРСИ

НАМАНГАН

Маълумотларни муҳофаза қилиш фанидан маърузалар курси Информатика ва АТ Касб таълими йыналиши талабалари учун мўлжалланган.

Тузувчи: **АЛИШЕР АНВАРОВ**

Ушбу маърузалар курси «Информатика ва АТ» кафедраси умумий йиғилишида муҳокама қилинган.
(__-мажлис баёни_____2006 й.)

,

1-МАЪРУЗА

I. МАЪЛУМОТЛАРНИ МУҲОФАЗА ҚИЛИШ

Муҳофаза системаси

(2 соат)

Ўқув модуллари

1. Маълумотларни муҳофаза қилиш тушунчаси.
2. Система хавфсизлигининг асосий принциплари.
3. Информацияни ҳимоя қилувчи системаларнинг моделлари .

Аниқлаштирилган ўқув мақсадлари.Талаба бу мавзуни тўла ўзлаштиргандан сўнг:

- ❖ Маълумотларни муҳофаза қилиш ҳақидаги тамойилларни билади;
- ❖ Система хавфсизлигининг асосий принципларини бўлакларга бўлиб, таъриф бера олади;
- ❖ Система ташкил этувчиларининг бутунлиги – система хусусиятларинини талқин эта олади;
- ❖ Информациянинг ишончлилиги принципларини қайси синфга мансублигини тасаввур эта олади;
- ❖ Система ташкил этувчисидан фойдаланувчанлиги ўртасидаги ўзаро алоқадорликни аниқлайди, боғланишларни таҳлил қила олади.

Таянч сўз ва иборалар:

Маълумот хавфсизлиги,информация ишончлилиги,ҳимоя моделлари,система хавфсизлиги, фойдаланувчи, критик информация, нокритик информация

Ҳозирги пайтда компьютер системаларида маълумотларни муҳофаза қилишни таъминлаш масаласи долзарб масалалардан бири бўлиб қолмоқда.

Муаммоли савол: Нокритик маълумотлар таркибига нималар киришини ыйлаб кыринг

Информациянинг ҳаммаси ҳам ҳимояга муҳтож эмас. Шунинг учун

информация ўз характерига кўра критик ва нокритик информацияга бўлинади.

Критик информация фойдаланувчининг шахсий ишлаб топган маълумотлари бўлиб, хизматчи информация, савдо-сотиққа оид сирларни ўз ичига олувчи информация ёки махфийликнинг турли кўриниш ёки шаклларига оид информация ва ҳ. бўлиши мумкин.

Бу бобда критик маълумотларни муҳофаза қилиш билан боғлиқ масалаларга эътибор қаратилади.

Айни пайтда компьютер техникасидан фойдаланувчиларнинг ҳаммаси ҳам бу масалаларнинг муҳимлигини англаб етмайдилар. Мамлакатимизнинг бозор иқтисодига ўтиши кўплаб фирма ва банкларнинг ташкил этилишига олиб келди, бу фирма ва банкларнинг самарали ишини эса компьютерларсиз ташкил этиб бўлмаслиги ҳаммага аён. Компьютер техникасидаги ҳар қандай бузилиш ўша фирма ёки ташкилот учун жиддий йўқотишларга олиб келиши мумкин. Шунинг учун ҳам маълумотларни муҳофаза қилиш масаласига жиддий ёндашмоқ зарур.

Системанинг хавфсизлиги деганда, унинг фойдаланувчи ёки эгаларига, турли қасддан ёки тасодифий қилинган таъсирлар натижасида, катта талофотлар етказишга бардош бера олиш хусусияти тушунилади. Бошқача сўз билан айтганда, система хавфсизлиги деганда унинг иш жараёнининг бир маромда кетишига халақит берувчи тўсиқлар, тасодифий ёки атайдан пухта ўйланган халақитлар, шунингдек, унинг ташкил этувчиларини ўғирлаш, ўзгартириш ёки бузишга қаратилган уринишларга қарши ҳимоя қобилияти тушунилади.

Системанинг хавфсизлигига 3 та асосий принципларни таъминлаш билан эришилади:

1) ***Система ташкил этувчиларининг бутунлиги*** – система хусусиятларининг унинг иш жараёнида ўзгармаслиги. Эксплуатация жараёнида система администратори томонидан бир қатор фойдали ўзгартиришлар ўтказилади ва бу ўзгартиришларнинг кам-кўсти тўлдирилиб охиригача етказилади (масалан -

WinNT системасига қўшимча тўлатувчи пакетни ўрнатиш), лекин бунда талаб қилинган хусусиятлар ўзгармайди - илгаригидек фойдаланувчини идентификация қилиш ва унинг системадаги ишини таъминлаши керак.

2) ***Информациянинг ишончлилиги*** – бу информациянинг шундай хусусиятики, бунда у системанинг фақат рухсат этилган ва текширувдан ўтган субъектларигагина (фойдаланувчилар, программалар, жараёнлар ва ҳ.) маълум бўлади.

3) ***Система ташкил этувчисидан фойдаланувчанлиги*** – фақат муаллиф субъектларнинг система ташкил этувчисидан ихтиёрий пайтда фойдалана олиш хусусияти. Бошқача айтганда, системанинг ҳар бир фойдаланувчиси идентификация қилинган ва фойдаланувчининг фойдаланиш даражасига мувофиқ ҳолда система ташкил этувчиларидан фойдаланишга рухсат этилган бўлиши керак. Бунда фойдаланиш даражаси хизматчининг хизмат мавқеи билан эмас, балки унинг қатъий функционал мажбуриятлари билан аниқланади.

Маълумки, ҳозирда компьютер ва компьютер системалари автоном ҳолда кам фойдаланилади. Улар одатда бир-бирлари билан локал, корпоратив ва глобал тармоқлар орқали боғланади. Компьютер системаларининг маълумотлар базасида катта ҳажмдаги информация шаклланган. Унинг йўқолиши, бузилиши ёки берухсат фойдаланилиши катта иқтисодий талофотларни келтириб чиқариши мумкин. Бундан четлашиш мақсадида берухсат фойдаланишлардан информацияни ҳимоя қилишнинг ҳар хил системалари қўлланилади.

Самарадорлиги юқори информацияни ҳимоя қилиш системасини ишлаб чиқиш аввало, бу системанинг концепциясини аниқлаш керак. Тадқиқот ўтказишда ва моделлаштиришда информацияни ҳимоя қилувчи восита юқори даражадаги ҳимоя қобилиятига эга эканлигини исботлаши лозим.

Информацияни ҳимоя қилувчи системаларнинг кўпгина моделлари ишлаб чиқилган. Бироқ энг кўп фойдаланиладиган моделлар қуйидагилардир:

1. **Белла ва Ла-Падула**; бунда фойдаланиш ҳуқуқини чеклаш воситаларини қуриш учун фаол субъектлар S ва пассив субъектлар Q тушунчалари киритилади. Ушбу ҳолда субъектлар фойдаланишнинг ҳар хил ҳуқуқла-

рига эга бўладилар. Бундай модел гоҳида “фойдаланиш ҳуқуқини чеклашнинг матрицали модели” деб ҳам юритилади;

2. **Денинг модели** – ҳар хил даражадаги махфийликка эга ҳужжатлар билан ишлашда информацияни ҳимоя қилиш воситасининг кўп сатҳли иерархик модели; бу ерда информацияни ҳимоя қилишнинг концентрлашган халқаси тушунчаси киритилади. Ички халқаларда – максимал махфийлик даражаси мавжуд бўлиб, ташқи қурилма (периферии)га яқинлашган сари махфийлик даражаси камаяди;
3. **Лендвер модели** - шундай компьютер тармоқларида фойдаланиладики, бундай тармоқдаги маълумотларни муҳофаза қилиш информацияни киритиш-чиқариш операцияларининг ҳимояси билан таъминланади.

Кўпгина реал вақт масштабида ишлайдиган мавжуд операцион системалар учун Белла ва Ла-Падула ҳимоя системаси концепциясидан фойдаланилади. Бу моделда фойдаланиш диспетчерининг қўлланилиши талаб этилади. Информацияни ҳимоя қилиш системасининг ўзи эса учлик кўринишида тасвирланади:

$$Zк(S,Q,P)$$

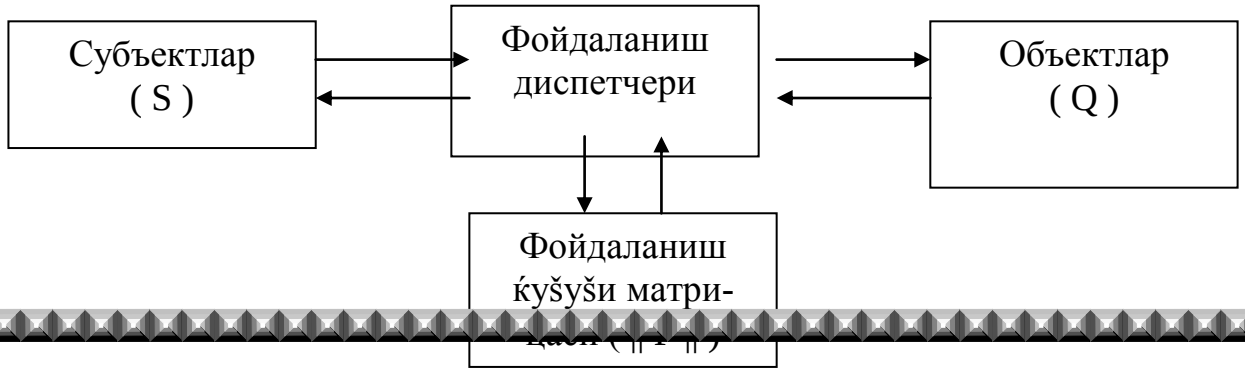
бу ерда:

S – фойдаланувчилар ва улар программаларидан иборат субъектлар ҳамда ўзидан-ўзи пайдо қилувчи жараёнлар, процедуралар ва б.;

Q – субъектлар билан сўров олиб бориши мумкин бўлган системанинг объект (ресурслари) тўплами; объектларга программалар, процедуралар, маълумотлар дисклари, томлар, файллар, алоҳида файл ёзувлари ва қурилмалар мансуб;

P – субъектларнинг объектлардан фойдаланиш ҳуқуқлари тўплами.

Информацияни ҳимоя қилиш системасининг умумий структураси 1-расмда келтирилган.



1-расм. Информацияни ҳимоя қилиш системасининг умумий структураси.

Битта процедура бир вақтда ҳам субъект, ҳам объект бўлиб чиқиши мумкин. Фойдаланиш ҳуқуқи битли векторлар билан аниқланади. Ҳар бир бит таъқиқлаш (запрет) ёки рухсат беришни аниқлайди: R, E, W, M, A, O; бу ерда R – ўқиш, E – таҳрирлаш, W – ёзиш, A – администратор, O – тўлиқ мулкдор (полний собственник).

Фойдаланишнинг минимал ҳуқуқи тўрт бит билан аниқланади: R, E, W, M. Фойдаланиш ҳуқуқини фойдаланиш администратори аниқлайди ва ҳеч қайси фойдаланувчи ||P|| матрицадан фойдаланиш имконига эга эмас, лекин уни ўзгартириши мумкин.

Кўпроқ ишончли ҳақиқийликка мос модел сифатида ўйин ҳимоя моделлари ифодаланади, яъни бундай моделларда камида иккита томон мавжуд бўлади. Биринчи томон информацияни ҳимоя қилиш системасини, иккинчи томон эса биринчи томон воситасида қурилган ҳимояни эгаллаш системасини қуради.

Шундай бўлишига қарамасдан кўпгина атакалар ва берухсат фойдаланишга бўлган ҳаракатлар пассив (яъни фойдаланувчи ҳақида информация йиғиш ва нусхалаш) ҳисобланади ва ўзида фаол атакага тайёр потенциал бузғунчини ошкор қилиши ҳам мумкин.

Ҳимоя системасини ишлаб чиқиш ҳимоя қилиниши лозим бўлган системанинг ўзини ишлаб чиқиш билан бирга олиб борилиши керак. Ҳимоя системасини яратиш тажрибаси қуйидаги асосий принципларни ажратиш имконини беради. Улар лойиҳалашда эътиборда бўлиши керак.

1. ***Ҳимоя механизмининг соддалиги.*** Бу принцип шунга асосланганки, лойиҳалашда ва эксплуатацияда юзага чиққан айрим хатолар фойдаланишнинг эътиборга олинмаган йўлларини аниқлашга имкон беради. Шунга асосан ҳимо-

янинг аппарат ва программ воситаларини синчиклаб тестлаш керак, бироқ амалиётда бундай текширувнинг фақат содда ва ихчам схемалар учун имконияти мавжуд.

2. *Информациянинг четга чиқиб кетиши мумкин бўлган ҳамма каналларнинг ёпиқлиги.* Бу принцип ҳар қандай объектга бўладиган ҳар қандай мурожаат ҳуқуқини (ваколатини) текширишга мўлжалланган ва ҳимоя системасининг асоси ҳисобланади.

Муаммоли савол: ***Информациянинг четга чи=иб кетиши мумкин былган щамма каналларни санаб ытинг.***

Бу принципни ҳисобга олган ҳолда, фойдаланишни бошқариш масаласи умумсистема сатҳида ечилиши лозим. Бунда ишга тушириш, бузилишлардан сўнг қайта тиклаш, ажратиш ва профилактик хизмат кўрсатиш каби иш режимлари эътиборга олинади. Маълумотларга бўладиган ҳар қандай мурожаат манбаини ишончли аниқлашни таъминлаши зарур.

3. *Ҳимоя механизмининг жиддий бўлмаган махфийлиги.* Кенг фойдаланишга мўлжалланган ҳимоя системасини амалга ошириш деталларини яшириши шарт эмас. Ҳимоя самарадорлиги потенциал бузғунчиларнинг маҳоратига боғлиқ бўлмаслиги керак. Чунки пароллар рўйхати ҳимоясини таъминлаш анча содда кечади. Ҳимоя механизмининг махфий эмаслиги зарур ҳолларда, унинг мутахассислар орасидаги кенг муҳокама субъекти бўлиши имконини беради.

4. *Фойдаланувчилар ҳуқуқ ва ваколатларининг тақсимланиши.* Компьютер тармоқлари ва системаларида бир қанча ҳимоя калитларининг мавжудлиги қачонки фойдаланишга бўлган ҳуқуқ бир қатор шартлар бажарилиши билан аниқланган ҳолатдагина қулайлик туғдиради.

5. *Минимал ваколат.* Ҳар қандай фойдаланувчи ва программа учун топширилган ишни бажариш учун зарур бўлган ваколатнинг минимал доираси

аниқланган бўлиши керак. Шунга кўра тасодифий бузилишларга сабаб бўладиган зарарлар маълум миқдорда камайиши мумкин.

6. ***Ҳимоя механизмининг максимал ихтисослаштирилганлиги.*** Фойдаланувчилар орасида информация алмашишини истисно қилиш мақсадида ҳимоя схемасини лойиҳалашда бир неча фойдаланувчилар учун умумий бўлган параметрлар ва ҳимоя механизми характеристикаси сонини минимумга олиб келиш мақсадга мувофиқ.

7. ***Психологик жозибадорлик.*** Ҳимоя системасини эксплуатация қилиш содда бўлиш лозим. Фойдаланувчининг ҳимоя системаси ҳақидаги тасаввурлари унинг фактларга асосланган имкониятлари билан қанчалик мос тушса, қўллаш жараёнида хатолар шунчалик кам бўлади. Айрим сунъий тилларнинг ҳимоя системасига мурожаат қилишда фойдаланилиши қўшимча хатолар манбаи бўлиб хизмат қилади. Юқорида санаб ўтилган принципларнинг айримларига асосланган системани қуришда уларни амалга оширишда сарфланадиган катта харажатлар билан боғлиқ жиддий тўсиқлар юзага келади. Шунинг учун ҳимоя системаларини лойиҳалашдаги муҳим фактор сифатида унинг иқтисодий самарадорлигини кўрсатиш мумкин.

Муаммоли савол: ***Щимоя системасининг =андай турларини учратгансиз?***

Шуни эсда тутиш лозимки, фаолиятнинг алоҳида тармоқлари (банк ва молия институтлари, информацион тармоқлар, давлат бошқарув системалари, мудофаа ва махсус хизмат структуралари) маълумотлар хавфсизлиги бўйича махсус чора-тадбирлар кўришни талаб қилади ва бу тармоқларда ечилаётган масалаларнинг характери ва аҳамиятига мос ҳолда информацион системанинг ишлаш ишончлилигига бўлган талаблар жуда юқори бўлади.

Маълумотларни муҳофаза қилиш масаласини кўриб чиқишда, даставвал, маълумотларни ўринсиз (номатлуб, номаъқул) ўзгартириш ёки йўқотишга олиб

келувчи рухсатсиз фойдаланиш ёки бузишнинг турлари билан танишиб чиқиш лозим. Бундай жиддий таҳдидлардан қуйидагиларни келтириш мумкин:

- жиҳоз (қурилма) ларнинг бузилиши: кабель системасининг бузилиши, электр манбаининг ўчиб-ёниши, диск системасининг бузилиши, маълумотларни архивлаш системасининг бузилиши, серверлар, ишчи станция

Муаммоли савол: ***Информациянинг четга чи=иб кетиши мумкин былган щамма каналларни санаб ытинг.***

- лар, тармоқ карталарининг бузилиши;
- программа таъминотининг нотўғри ишлаши оқибатида келиб чиқадиган информация йўқолиши, программа таъминотининг носозлиги натижасида маълумотларнинг ўзгариб кетиши ёки йўқ бўлиб кетиши, системанинг компьютер вируслари билан зарарланиши натижасида маълумотларнинг йўқолиши ва ҳ.;
- рухсатсиз фойдаланиш билан боғлиқ йўқотишлар: информациядан рухсатсиз нусха олиш, йўқотиш ёки қалбакилаштириш, махфий, сир тутилиши лозим бўлган информацияни бегона кишиларга таништириш;
- архив маълумотларини нотўғри сақлаш билан боғлиқ йўқотишлар;
- хизматчи шахс ёки фойдаланувчининг хатолари: маълумотларни ўзи билмаган ҳолда ўзгартириш ёки йўқотиб юбориш, маълумотларнинг йўқолишига ёки бузилишига олиб келувчи программа ёки аппарат таъминотидан нотўғри фойдаланиш.

Бу таҳдидлардан келиб чиқиб, информацияни ҳимоялашнинг барча турларини қуйидаги 3 та синфга бўлиш мумкин:

- ***физик ҳимоялаш воситалари:*** кабель системасини, электр манбаи системасини ҳимоялаш воситалари, ҳимоялашнинг аппарат воситалари, архивлаш, дискли массивлар ва ҳ.;

- ***ҳимоялашнинг программа воситалари:*** антивирус программалари, ваколатларни (фойдаланиш имкониятларини) чеклаш системаси, фойдаланишни назорат қилувчи программа воситалари;
- ***ҳимоялашнинг маъмурий чора-тадбирлари:*** бинога киришни назорат қилиш, фирма ёки ташкилотнинг хавфсизлигини таъминлаш стратегиясини ишлаб чиқиш, фавқулодда ҳолатларда ҳаракат қилиш режаларини тузиб чиқиш ва б..

Бундай синфлаш шартли эканлигини унутмаслик лозим, чунки Ҳозирги замонавий технологиялар аппарат-программ ҳимоя воситалари билан бир йўналишда ривожланиб бормоқда. Бундай аппарат-программ воситаларидан, хусусан, вируслардан ҳимояланиш, фойдаланишни назорат қилиш ва ҳ. кенг тус олмоқда.

Банкларда нақд пуллар йиғилгани каби компьютерда ҳам информациянинг тўпланиши ҳам информацияни ҳимоялаш мақсадида назоратни янада кучайтиришни талаб қилади.

Юридик масалалар, хусусий сир, махфий маълумотлар, миллий хавфсизлик - буларнинг барчаси тижорат ва ҳукумат ташкилотларида ички назоратни кучли ташкил этишни талаб қилади. Бу йўналишдаги ишлар янги «Маълумотларни муҳофаза қилиш» фанининг пайдо бўлишига олиб келди. Маълумотларни муҳофаза қилиш бўйича мутахассис ташкилотда йиғилган информациянинг бутунлиги, махфийлиги, фойдаланишга яроқлилигини таъминлашга қаратилган маълумотларни муҳофаза қилиш системасини ишлаб чиқиш, йўлга қўйиш ва ишлатиш ишларига масъулдир. Унинг вазифаларига информацион ресурсларни физик (техник воситалар, алоқа каналлари ва узоқлаштирилган компьютерлар) ҳамда мантиқий (маълумотлар, амалий программалар ва операцион системалар) ҳимоялашни таъминлаш киради.

Информацияни ҳимоялаш системасини яратиш мураккаблиги шундаки, маълумотлар компьютердан ўғирланиши билан бир вақтда ўз жойида қолиши

ҳам мумкин, яъни баъзи маълумотларни йўқотиш ёки ўзгартириш эмас, балки бутунича нусха кўчириб олиб кетишнинг ўзи кифоя қилади.

Маълумотларни муҳофаза қилишни таъминлаш - қиммат ҳамда катта сарф-харажатларни талаб қиладиган иш бўлиб, воситаларни сотиб олиш ёки ўрнатишга қанча сарф-харажат қилинмасин, мос таъминот системасининг ишга лаёқатли ҳолатини ва оқилона хавфсизлик чегарасини малакали аниқлаш шунчалик қийин бўлади. Агар локал тармоқ умумий фойдаланилувчи кўп сонли информация файллари, қимматбаҳо рангли принтерлар ёки лицензион программа воситаларидан биргаликда фойдаланиш мақсадида ишлаб чиқилган бўлса, у ҳолда информацияни ҳатто минимал шифрлаш ёки дешифрлаш ҳам талаб қилинмайди.

Информацияни ҳимоялаш воситаларини лойиҳалаш, сотиб олиш ёки ўрнатишни етарлича таҳлилларни олиб бормасдан туриб амалга ошириш керак эмас. Таваккални таҳлил қилиш кўплаб факторлар (ишнинг бузилишининг пайдо бўлиши, ишнинг бузилишининг пайдо бўлиш эҳтимоллиги, тижорат йўқотишлардан зарар кўриш, системанинг тайёргарлиги коэффициентининг камайиши, жамоат муносабатлари, юридик муаммолар) нинг объектив баҳоларини бериши ҳамда хавфсизликнинг мос турларини ва даражаларини аниқлаш учун информация тақдим этиши шарт. Тижорат ташкилотларининг барчаси маълум даражада кўп бўлган критик корпоратив информацияни катта-катта ҳисоблаш системаларидан олиб, очиқ система воситаларига узатишда хавфсизлик системасидан фойдаланиш ва уни йўлга қўйишда янги, ҳали номаълум бўлган мураккаб муаммоларга дуч келадилар. Ҳозирда кўплаб ташкилотларда тижорат маълумотларини бошқариш учун юқори қувватли, тақсимланган маълумотлар базаси ва клиент/сервер технологиясидан фойдаланилмоқда. Тақсимланишнинг ўсиши билан бирга бу маълумотларга рухсатсиз кириш ва уларни бузиш имкониятлари ҳам кўпайиб бормоқда.

Компьютер системасининг хавфсизлигига эришиш жараёнида системага таъсир этиши мумкин бўлган барча ҳолатларни таҳлил ва прогноз қилиш керак.

Системага кўрсатиладиган таъсирлар 2 турга фарқланади - ***тасодифий*** ва ***атайдан (қасддан) қилинган таъсирлар***.

Фойдаланилган адабиётлар рўйхати

1. С.Петренко ,М.Мамаев «Технологии заҳитў в Интернете» Издательский дом «Питер» , Санкт-Петербург, 2002 г.
2. Турский А. , Панов С «Заҳита информации при взаимодействии корпоратив-нўх сетей в Интернет» , ФиС, Москва, 2003 г.
3. Кошелев А.»Заҳита сетей и firewall» КомпьютерПресс, 2000 г.

2-МАЪРУЗА

Тасодифий таъсирлар ва улардан информацияни муҳофаза қилиш усуллари. **(2 соат)**

Ўқув модуллари

4. Системага тьалафот етказадиган тасодифий таъсирлар тушунчаси.
5. Диск ва каналларни резервлаш
6. Информацияни ҳимоя қилувчи системаларнинг моделлари .

Аниқлаштирилган ўқув мақсадлари.Талаба бу мавзуни тўла ўзлаштиргандан сўнг:

- ❖ Маълумотларни муҳофаза қилиш ҳақидаги тамойилларни билади;
- ❖ Система хавфсизлигининг асосий принципларини бўлакларга бўлиб, таъриф бера олади;
- ❖ Система ташкил этувчиларининг бутунлиги – система хусусиятларинини талқин эта олади;
- ❖ Информациянинг ишончлилиги принципларини қайси синфга мансублигини тасаввур эта олади;
- ❖ Система ташкил этувчисидан фойдаланувчанлиги ўртасидаги ўзаро алоқадорликни аниқлайди, боғланишларни таҳлил қила олади.

Таянч сўз ва иборалар:

Маълумот хавфсизлиги,информация ишончлилиги,ҳимоя моделлари,система хавфсизлиги, фойдаланувчи, критик информация, нокритик информация

Тасодифий таъсирлар – бу системага талофот етказадиган ёки уни умуман ишдан чиқарадиган таъсирлар. Масалан, электр манбаининг бузилиши, қурилманинг ишдан чиқиши, ёнғин, сув босиши ва шу кабилар. Тасодифий таъсирлар натижасида информация бузилиши ёки йўқолиши мумкин. Шунинг учун қуйидаги информацияни ҳимоя қилиш ва тиклаш воситаларидан фойдаланиш мумкин:

Кўзгули дисклар (зеркальнўе диски) – булар дискларнинг физик зарарланиши билан боғлиқ йўқотишларнинг олдини олиш учун дискларни резервлаш мақсадида фойдаланиладиган дисклар.

Дискларни резервлаш учун битта диск контроллерига 2 та мутлақо бир хил винчестер уланади ва операцион система шунга мувофиқ мослаштирилади. Сўнгра асосий дискдаги барча информация ***кўзгули диск*** деб номланувчи иккинчи дискда иккилантирилади.

Асосий диск зарарланганда махсус процедуралар ёрдамида кўзгули дискдан барча маълумотларни қайта тиклаш мумкин. қўшимча равишда диск йўлакчаларининг «қайноқ» резервлаш ҳам ишлатилади. Дискда «қайноқ» резервлаш соҳаси ажратиб олинади. Агар иш жараёнида дискда нуқсонли йўлакча топилса, бу йўлакча резервлаш соҳасидаги йўлакча билан алмаштирилади.

Диск ва каналларни резервлаш - кўзгули дисклардан фойдаланишда иккала дискнинг ҳам канали, контроллери ва ток манбаи зарарланиш эҳтимоли мавжуд. Баъзи операцион системалар (масалан, NetWare) канални бутунлай резервлай олиш имкониятига эга, мос равишда иккита дискка уланган контроллердан фойдаланиши мумкин. Бу контроллер ва дискларни ток билан таъминлаш учун иккита ток манбаи керак.

Серверни «қайноқ» резервлаш – кўзгули дискдан маълумотларни тиклаш диск хотира ҳажмига боғлиқ равишда бир неча соатлаб вақтни олиши мумкин. Баъзида тармоқда ишнинг бундай узоққа чўзилишини кутиб бўлмайди. Бундай ҳолларда серверларни «қайноқ (горячее)» резервлашдан фойдаланиш маъқул. Серверларни қайноқ резервлашнинг маъноси шуки, бунда иккита сервер MSL-адаптер (Microred Server Link) деб аталувчи махсус адаптер ёрдамида тезлаштирилган алоқа линияси орқали ўзаро бир-бирига уланади. Бу адаптерлар ўзаро 33 м гача узунликдаги коаксиаль кабель ёки 4 км гача узунликдаги оптик толали кабель ёрдамида бириктирилади. Бу усулда турли серверларни турли биноларга жойлаштирган ҳолда, ҳаттоки биноларнинг бирортасидан ёнғин чиққан шароитда ҳам система ишининг ишончлилиги ва мустаҳкамлигини таъминлаш мумкин.

Битта сервернинг ишдан чиқиши тармоқ ишининг тўхтаб қолишига олиб келмайди, чунки бунда автоматик равишда иккинчи резерв-сервер ишга тушади. Юқори тезликдаги алоқа каналидан фойдаланиш эвазига резерв-сервер диски ҳам асосий дискдаги файлларни ўзида сақлайди, шунинг учун маълумотларни тиклаш каби ортиқча амалларни бажаришга ҳеч ҳам хожат қолмайди.

Узлуксиз энергия манбаи – агар тармоқнинг иши ёки сервердаги маълумотларнинг ишончли сақланишига катта талаб қўйиладиган бўлса, у Холда узлуксиз энергия манбаи қурилмасидан фойдаланмоқ жоиз. Бу қурилма шунчаки маълум вақт давомида серверни ток билан таъминловчи аккумулятор эмас. Бу қурилма махсус адаптер орқали серверга уланади. Агар ток манбаи бўйича узилиш содир бўлса, қурилма серверга бу ҳақда сигнал беради ва шу сигнал буйича сервер секин-аста, маълумотлар йўқолишининг олдини олган ҳолда, ўз ишини тамомлайди.

Мустаҳкамлаш учун саволлар :

1. Маълумотлар муҳофазаси нимани англатади ?
2. Диск ва каналларни резервлаш тушунчасини изоҳланг.
3. ***Тасодифий таъсирлар тушунчасини айтиб беринг.***
4. ***Узлуксиз энергия манбаларини қандай турларини биласиз?***

Фойдаланилган сайтлар рўйхати

- www.securityfocus.com-портал: материалў по безопасности
- www.sans.org-Институт SANS: статьи по безопасности, проектў
- www.xforce.iss.net-база даннўх уязвимостей, материалў по безопасности
- www.packetfactory.net-сайт разработчиков библиотеке
- blacksun.box.sk/ tutorials.html-аспектам сетевой безопасности работў с сетевўх сервисов.

3-4-МАЪРУЗАЛАР

Қасддан қилинган таъсирларнинг турлари ҳамда улардан информацияни ҳимоялаш усуллари

(4 соат)

Ўқув модуллари

7. Системага қасддан қилинган таъсирлар тушунчаси.
8. Рухсатсиз кириш (фойдаланиш)
9. Информацияни ҳимоя қилувчи системаларнинг моделлари .

Аниқлаштирилган ўқув мақсадлари.Талаба бу мавзуни тўла ўзлаштиргандан сўнг:

- ❖ Маълумотларни муҳофаза қилиш ҳақидаги тамойилларни билади;
- ❖ Система хавфсизлигининг асосий принципларини бўлакларга бўлиб, таъриф бера олади;
- ❖ Система ташкил этувчиларининг бутунлиги – система хусусиятларинини талқин эта олади;
- ❖ Информациянинг ишончлилиги принципларини қайси синфга мансублигини тасаввур эта олади;
- ❖ Система ташкил этувчисидан фойдаланувчанлиги ўртасидаги ўзаро алоқадорликни аниқлайди, боғланишларни таҳлил қила олади.

Таянч сўз ва иборалар:

Маълумот хавфсизлиги,информация ишончлилиги,ҳимоя моделлари,система хавфсизлиги, фойдаланувчи, критик информация, нокритик информация

Системага қасддан қилинган таъсирлар – бу система иш жараёнининг бир маромда келишига атайдан қилинган тўсқинлик, шунингдек унинг ташкил этувчиларини ўғирлаш, ўзгартириш ёки бузишга қаратилган уринишлардир. қуйида маълумотларни муҳофаза қилишга қасддан қилинган таҳдидларнинг таснифи ва қисқача тавсифи келтирилган. Бу тасниф хавфсизлик администратори тез-тез дуч келадиган қасддан қилинган таъсирларнинг асосий турларини ажрата олиш ва улардан ҳимояланиш усулларидан фойдаланиш учун керак.

Рухсатсиз кириш (фойдаланиш) (РК, РФ) – бу компьютер бузғунчилигининг энг кенг тарқалган тури. Бу ташкилотнинг хавфсизлик сиёсатига мувофиқ киришга рухсати йўқ фойдаланувчининг бирор объектдан фойдаланиш учун кириш билан боғлиқ ҳаракатдир. Бу ерда асосий муаммо “Кимда қайси маълумотлар жамғармасидан фойдаланишга рухсат бор? Кимда бу рухсат йўқ?” саволларига жавоб топишдадир. Бошқача айтганда “рухсатсиз” атамасини аниқлаш керак.

Таъсирининг характерига кўра РК (ёки РФ) системанинг хатоларидан фойдаланувчи фаол таъсирлар бўлади. РК одатда, бевосита маълумотлар жамғармасига мурожаат қилади ёки РК қонунийлаштириш мақсадида рухсат этилган кириш тўғрисидаги информацияга таъсир этади. Тармоқнинг ҳар қандай объекти РКга йўлиқиши мумкин. Ҳар қандай объектга РК стандарт ёки махсус программа воситалари орқали амалга оширилиши мумкин.

РК амалга ошириши маълум маънода компьютер тармоғини ташкил этиш, ундаги хавфсизлик сиёсати, ўрнатилган ҳимоя воситаларининг имкониятлари, шунингдек, администратор ва операторнинг виждонига боғлиқ.

РКни амалга оширишнинг 2 та усули мавжуд:

- биринчидан, ҳимоя системасини чуқур ўрганиб барбод этиш, яъни унга турли таъсирлар кўрсатиб унинг иш жараёнини тўхтатиш. Бу жуда мураккаб ва қийин, ҳамма вақт ҳам амалга ошавермайдиган, бироқ самарали ишдир;
- иккинчидан, нима эътибордан четда эканлигини кузатиш, яъни бузғунчига керакли қайси маълумотлар жамғармаси фойдаланишга

очиқ ёки администратор эътиборидан четда эканини аниқлаш. Буни ҳам РК деб аташ мумкин ва амалга ошириш осон, лекин бу ишлар маълум бўлиб қоладиган бўлса, ҳимояланиш қийин. Бундай турдаги РКга паролни топиш, паролни тузиш қоидаларини бузиш, инсон исмидан, такрорланувчи символлардан парол сифатида фойдаланиш кабиларни ҳам киритиш мумкин. РКнинг кўпчилик бузувчи ҳолатларига пухта ўйламасдан ҳимоя воситасини танлаш, уни нотўғри ўрнатиш ёки мослаштириш, иш жараёнини яхши назорат қилмаслик, шунингдек маълумотларнинг ҳимоясига совуққон муносабатда бўлиш кабилар киради.

Имтиёзлардан ноқонуний фойдаланиш – атаканинг бу усулини қўлловчи бузғунчилар одатда, штатдан ташқари режимда ишловчи штат программа таъминоти (системали ёки амалий ПТ) дан фойдаланадилар. Амалда ҳар қандай ҳимояланган система фавқулодда вазиятларда ишлатилувчи, қурилма ёки воситалар бузилганда, мавжуд хавфсизлик сиёсатининг бузилиши шароитида ишлай олувчи, бу вазифаларни бажара олувчи воситаларга эга бўлади. Баъзи ҳолларда фойдаланувчи системанинг барча наборларига кириш имкониятига эга бўлиши керак. Бундай воситалар керак, лекин фавқулодда хавфли бўлиши мумкин. Бу воситалар одатда, администраторлар, операторлар, система программистлари ва бошқа махсус вазифаларни бажарувчи фойдаланувчилар томонидан фойдаланилади.

Бундай воситалардан фойдаланишни камайтириш мақсадида, кўпчилик ҳимоя системалари уларнинг вазифаларини имтиёзлар набори ёрдамида амалга оширади – маълум вазифани бажариш учун маълум имтиёзлар талаб қилинади. Бундай ҳолларда ҳар бир фойдаланувчи ўзининг имтиёзлари наборига эга бўлади, оддий фойдаланувчи – минимал, администраторлар – максимал (имтиёзлар минимуми принципига мувофиқ) имтиёзга эга бўлади. Ҳар бир фойдаланувчи имтиёзлар набори унинг атрибутлари ҳисобланади ва ҳимоя системаси томонидан муҳофаза қилинади. Имтиёзларни рухсатсиз ишғол қилиш, шу тарзда, маълум вазифаларни рухсатсиз бажариш имкониятларини беради. Бу РК (ху-

сусий ҳолда), маълум программаларни ишга тушириш ва ҳатто системани реконфигурация қилиш бўлиши мумкин.

Табиийки, бундай шароитларда имтиёзларнинг кенгайтирилган набори – бу ҳар қандай бузғунчининг ўйлаб юрган орзуси. Бу эса унга амалда ҳар қандай ҳаракатларни амалга ошириш, шу билан бирга, ҳатто барча турдаги назорат чора-тадбирларини кўриб айланиб чиқиш имконини беради. Имтиёзлардан нотўғри фойдаланиш натижасида келиб чиқаётган бузғунчиликлар бирор объект ёки бутунлай системага кириш мақсадида қилинаётган актив таъсирдир.

Имтиёзларни ноқонуний ишғол қилиш ҳодисаси ё ҳимоя системасининг ўзида бирор хато пайдо бўлиши, ё система хусусан имтиёзларни бошқаришдаги бепарволик натижасида содир бўлиши мумкин. Ҳимоя системасининг бошқарув қоидаларига, имтиёзлар минимуми принципларига қатъий риоя қилиш билан бу хилдаги бузилишларнинг олдини олиш мумкин.

“***Яширин каналлар***” – система хавфсизлик сиёсатини бузувчи, система жараёнлари ўртасида информациянинг ўтиш йўли бўлинган ҳолда (с разделением) информацияга кириш муҳитида фойдаланувчи ўзини қизиқтирган информация билан ишлашга рухсат ололмаслиги мумкин, лекин бунинг учун айланма йўлларни ўйлаб топиш мумкин. Системадаги ҳар қандай ҳаракат амалда унинг бошқа элементларига маълум маънода таъсир кўрсатади. Бу боғланишларни етарлича кузатиш ва ўрганиш натижасида маълумотлардан бевосита ёки билвосита фойдаланиш имкониятига эга бўлиш мумкин.

“Яширин каналлар” турли йўллар билан ташкил этилиши мумкин, масалан программа закладкалари. Масалан, программист автоматлаштирилган системани яратиш жараёнида ўзини қизиқтирувчи маълумотларни олиш йўлларини олдиндан назарда тутиши мумкин. Бундай ҳолда программа яширин тарзда программист билан алоқа каналини ўрнатади ва унга талаб қилинган хабарларни узатиб туради.

“Яширин каналлар” дан фойдаланган ҳолда атака қилиш информация махфийлигига путур етказади, таъсир характери бўйича пассив ҳисобланади, яъни бузғунчилик фақат маълумот узатишда рўй беради. Яширин каналларни

ташкил этишда штатдаги программа таъминотидан фойдаланилса, махсус ишлаб чиқилган <троя> ёки вирус программаларидан шундай фойдаланилади. Атака асосан программа йўли билан амалга оширилади.

Информацияни яширин канал бўйлаб узатишга мисол қилиб, масалан, “TOTAL” сўзи ўрнига “TOTALS” сўзи ишлатилган якуний ҳисоботни олиш мумкин – бунда программист шундай қиладики, маълум шароитларда программа ўзи бирор сўзни аниқлаб, уни бошқасига алмаштириб қўяди. Бу каби яширин каналлар сифатида иккита сўз орасидаги пробеллар сони, каср сонда вергулдан кейинги учинчи ёки тўртинчи рақам ва ҳ. (яъни ҳеч кимнинг эътиборини тортмайдиган таъсир) дан фойдаланиш мумкин. Яширин канал бўлиб, шунингдек, бирор маълумотлар наборининг бор-йўқлиги, бу набор ўлчами, яратилган санаси, ўзгартирилган санаси ва ҳ. тўғрисидаги информацияни узатиш ҳам хизмат қилиши мумкин.

Системанинг икки жараёни ўртасидаги боғланишни ташкил қилишнинг кўпгина усуллари мавжуд. Бундан ташқари, кўпгина ОС лар таркибида (бошқарув остида) шундай воситалар борки, улар программистлар ва фойдаланувчилар ишини анчагина енгиллаштиради. Асосий муаммо шундаки, рухсат этилмаган “яширин каналлар”ни рухсат этилганлардан, яъни хавфсизлик сиёсати томонидан таъқиқланганларидан ажратиш жуда қийин. Охир оқибатда буни “яширин каналлар”нинг ташкилотга етказувчи талофотларидангина аниқлаш мумкин. “Яширин каналлар”нинг алоҳида, ўзига хос хусусияти қуйидагилардан иборат:

- паст даражадаги ўтказиш қобилияти (улар орқали фақатгина кичик миқдордаги информацияни узатиш мумкин);
- уларни ташкил қилишдаги қийинчиликлар;
- одатда, улар томонидан етказиладиган катта бўлмаган талофотлар.

Шунингдек, улар кўзга кўринмас, сезилмайдиган бўлишади, шунинг учун уларга қарши камдан-кам ҳолларда махсус ҳимоя чоралари қўлланилади. Одатда, пухта ишлаб чиқилган хавфсизлик сиёсатининг ваколатлари етарли бўлади.

«Маскарад» (инглизча «mask» - ниқоб сўзидан олинган) - деганда бир фойдаланувчининг бошқа фойдаланувчи номидан ҳаракат қилиши тушунилади. Бунда бу ҳаракатлар бошқа фойдаланувчи учун рухсат этилган бўлади. Бу ерда бузғунчилик бировнинг ҳуқуқ ва имтиёзларини ўзлаштириш асосида ташкил этилади.

Бундай бузғунчиликлар муғомбирлик ёки моделлаштириш деб ҳам аталади. «Маскарад»нинг асосий мақсади – бирор ҳаракатни бошқа фойдаланувчи номи остига беркитиш ёки бошқа фойдаланувчининг маълумотлар омборига кириш учун ёки унинг имтиёзларидан фойдаланиш мақсадида, унинг ҳуқуқ ва имтиёзларини ўзлаштиришдан иборат.

«Маскарад» система ҳимоясини фаол бузиш усулидир, у билвосита таъсир бўлиб, бошқа фойдаланувчиларнинг имкониятлари воситасида амалга оширилади. Унга мисол қилиб, системага бошқа фойдаланувчи номи ёки пароли билан киришни кўрсатиш мумкин, яъни бунда система бузғунчилик бўлганини аниқлай олмайди. Бунда «Маскарад»дан олдин эса системани бузиш ёки паролни ўғирлаш жараёни амалга ошади. Яна бир мисол, иш жараёнида бошқа фойдалнувчи номини ўзлаштиришдир. Буни операцион системалар воситалари ёрдамида (баъзи операцион системаларда фойдаланувчи идентификаторини иш жараёнида ўзгартириш имконияти мавжуддир) ёки маълум жойдаги маълум информацияни ўзгартира оладиган программалар (масалан, паролларни топиш, системага кириш паролларини ўғирлаш программалари) ёрдамида амалга ошириш мумкин, ва бунинг натижасида фойдаланувчи бошқа фойдаланувчи исмини ўзлаштиради. Бундай амаллар одатда,, система имтиёзларига эга бўлган ҳолда ёки системадаги бирор хатодан фойдаланган ҳолда амалга оширилади. Шунингдек, компьютер тармоғида бошқа фойдаланувчи томонидан маълумот узатиш ҳам «Маскарад» деб аталади. Идентификаторни ўзгартириш усуллари турлича бўлиши мумкин, одатда,, улар тармоқ протоколлари хусусиятлари ва хатолари билан аниқланади. Шунга қарамай, қабул қилувчи узелида маълумот тўғри маълумот каби қабул қилинади ва бунинг натижасида тармоқ иши жиддий зарар кўриши мумкин.

Бундай ахборотларга, асосан, тармоқ конфигурациясининг ўзгаришига таъсир этувчи-бошқарувчи ахборотлар ёки имтиёзли амалларни бажаришга олиб борувчи ахборотлар киради.

«Маскарад» - бу корхона ишини бузиш, информация оқимини ва тармоқ (ёки система) конфигурациясини ўзгартириш каби оғир оқибатларни келтириб чиқарувчи, аҳамиятга молик бузғунчиликдир. Уни бартараф этиш учун аутентификация ва идентификациянинг ишончли усулларидан фойдаланиш, системани бузишга уринишлардан блокировка қилиш, системага киришни назорат қилиш лозим. Шунингдек, система журналидаги «Маскарад» тўғрисида гувоҳлик берувчи барча ҳодисаларни эътиборга олиш ва аҳамият бериш зарур.

«***Чиқинди йиғиш***» (Сборка мусора). Иш тугагандан сўнг ишланаётган информация ҳамма вақт ҳам хотирадан тўлалигича ўчиб кетмайди, маълум қисм маълумотлар оператив хотира, ташқи хотира қурилмалари ёки бошқа хотира қурилмаларида қолади. Бу маълумотлар токи хотира қурилмасидан ўчириб юборилмагунча ёки устидан бошқа маълумот ёзилмагунча хотира қурилмасида туради, бироқ ўчириб юборилгандан сўнг ҳам маълумотларнинг маълум қолдиқлари сақланиб қолади. Бундай пайтда бу қолган қолдик маълумотларни ўқиб олиш анча қийин бўлсада, уни махсус программалар ёрдамида амалга оширса бўлади. Натижада йиғилган қолдиқлардан асосий маълумотни қисман тиклаш имконияти пайдо бўлади. Бу жараён «чиқиндиларни йиғиш» деб номланади. Бу муҳим ва махфий сақланаётган информациянинг четга чиқиб кетишига олиб келиши мумкин.

«Чиқинди йиғиш» автоматлаштирилган система объектларига бевосита фаол таъсир этиб, улардаги информация махфийлигига путур етказади.

Бу таъсирлардан ҳимояланиш учун компьютер аппаратураси ёки операцион системасида ёки яна бирор бир қушимча аппарат-программа воситаларда амалга оширилган махсус механизмлардан фойдаланилади. Бундай механизмларга мисол, ўчирувчи намуна ва тўлалик белгиси ишлатилади.

Ўчирувчи намуна – бу файлдан бўшаган жойга ёзувчи бир қанча битлар кетма-кетлиги. Хотиранинг ҳар бир қисми бўшатилгандан сўнг, хотирадан

маълумот ўчирилгандан сўнг, хавфсизлик бошқарувчиси (администратори) автоматик равишда бу бўшатилган ўринга битлар кетма-кетлигини ёзиш фаолиятини олиб боради ва бунинг натижасида ўчирилган маълумотлар физик сақлаш муҳитидан ҳам батамом йўқотилади.

Тўлалик белгиси - бу хотиранинг ёзиш учун жўнатилган, лекин ҳали ёзиб улгурилмаган (ёзилмаган ёки фойдаланилмаган) участкаларини ўқишдан қайтаради. Фойдаланилган хотира адресига юқори чегара қўйилади ва хотира участкасининг тўлиб қолган белгиси ўрнатилади. Бу фавқулодда фойдаланиладиган (камдан-кам учрайдиган киришли) кетма-кет файлларни ҳимоялаш учун ишлатилади. (бу файллар - таҳрирлагичларнинг якунловчи файллари, компиляторлар, компоновшиклар ва ҳ.). Индексли ва бўлинувчи кетма-кет файллар учун бу усул «жойлаштираётиб ўчириш» деб номланади, хотиранинг уни жараён учун ажратаётган пайтда тозаланади.

Системани бузиш - бу рухсатсиз кириш параметрлари билан, яъни фойдаланувчи номи ёки пароли билан система ичига қасддан суқилиб кириш. Системани бузиш бу фаол системага тўла равишда қасддан қилинган таъсир бўлиб, одатда, интерактив режимда юз беради. Фойдаланувчи исми сир бўлмасада, "ўлжа" сифатида асосан парол танланади. Паролни очиш турлича бўлиши мумкин: эҳтимолли паролларни танлаб кўриш, бошқа фойдаланувчи паролидан фойдаланилган "Маскарад", имтиёзларга эга бўлиш ва ҳ. Шунингдек, кириши программасининг хатоларидан фойдаланган ҳолда ҳам системани бузиш мумкин. Шунда қилиб бузишда ҳимоялаш вазифаси асосан кириш программасининг зиммасига юклатилади. Паролни ва номни киритиш алгоритми, уларни шифрлаш, паролларни сақлаш ва ўзгартириш қоидаларида хато бўлмаслиги керак. Системани бузишга қаршилик кўрсатиш ҳам мумкин, масалан, паролни нотўғри киритишга бўлган уринишлар сонини блокировка ёрдамида ёки бузилиш содир бўлганда операторни хабардор қилиш орқали чеклаш.

Шунингдек хавфсизлик администратори системанинг фаол фойдаланувчиларини доим назорат қилиб туриши лозим: уларнинг исми-шарифи, иш характери, кириш-чиқиш вақти ва ҳ. дан хабардор бўлиб туриш керак. Бундай

ҳаракатлар системани бузилганлиги тўғрисидаги фактни олиш ва аниқлаштириш ҳамда зарур чора-тадбирларларни қўллашда катта ёрдам беради.

Туйнуклар - программа модулига яшириш, хужжатсиз кириш нуқтаси. Туйнук асосан программага ишни енгиллаштириш мақсадида созлаш босқичида қўйилади: программа модули турли жойлардан чақирилади, бу эса унинг алоҳида қисмларини мустақил созлаш имконини беради. Бироқ кейинчалик программист туйнукни йўқотишни унутиб қўяди ёки уни нотўғри блокировка қилиши мумкин. Бундан ташқари, туйнук бурилган программа модулини кейинчалик бошқа модуллар билан боғлаш мақсадида шу программа модулига қўйилади, лекин кейинчалик шарт-шароитнинг ўзгариши билан бу нуқта (яъни туйнук) керак бўлмай қолади. Туйнукнинг мавжудлиги программани ностандарт кўринишда чақириш имконини беради, яъни бу программа ҳимоя системаси назоратида бўлиши мумкин (бундай шароитда программа маълумотларни, система муҳитини ва ҳоказоларни қандай қабул қилиши номаълум). Шунингдек, бундай пайтда бу программанинг ҳатти-ҳаракатини ҳамма вақт ҳам прогноз қилиб бўлмайди. Туйнук бу бирор лойиҳани ишлаб чиқишда содир бўладиган хатоликлар натижасида пайдо бўладиган таҳдид бўлиб, ундан фойдаланиш ўша лойиҳа ёки программа пакетининг ўзига боғлиқ бўлади. Шунинг учун бу таҳдидни синфлаш мураккаб жараён ҳисобланади.

Хулоса қилиб айтганда туйнукларнинг пайдо бўлиш сабабларини қуйидагича кўрсатиш мумкин:

- туйнукларни йўқотишни унутиш;
- туйнуклардан кейинчалик программани созлашда фойдаланиш;
- туйнукдан ишлаб чиқилаётган программа ва тайёр программа (яъни туйнук қўйилган программа) ўртасида кўприк сифатида фойдаланиш;
- берилган программани ўрнатгандан сўнг бу программага махфий назоратни ташкил қилиш.

Бу ерда дастлабки ҳолат - аввалдан кутилмаган адашиш бўлиб, ҳимоя системасида катта бўшлиқ ёки очик туйнук пайдо бўлишига олиб келади. Иккинчи ва учинчи ҳолатлар хавфсизлик системаси учун жиддий синов вазифасини

ўтайди, бу ҳолатда хавфсизлик системаси информацион системани бу хавфдан огоҳ қила олмайди. Тўртинчи ҳолат эса - бу берилган программадан фойдаланган ҳолда олдиндан бирор мақсадни кўзлаб қилинган таъсирнинг биринчи қадамидир.

Шуни эсда тутиш лозимки, программанинг ҳар қандай хатоси ҳам туйнук ҳисобланмайди. Туйнук бу программани созлаш, тузатиш ва таъмирлашда кенг ишлатиладиган механизмдир, ҳаттоки у бирор мақсадда ишлатилсада, салбий характерга эга бўлавермайди. Яна таъкидлаш лозимки, агарда туйнук очиқ қолдирилса ва назорат чоралари кўрилмаса, у ҳолда бу система учун жиддий хавфдир.

Туйнуклардаги энг катта хавф - бу операцион системалардаги туйнуклардир, бунда уларни топиш жуда қийин кечади. Агар берилган программада туйнук мавжудлиги олдиндан маълум бўлмаса, уни топиш учун программа килобайт, мегабайт кодларини ишлашга тўғри келади. Бунга эса ҳақиқатдан олиб қараганда, деярли эришиб бўлмайди. Шунинг учун туйнукларни топиш бу тасодифий жараёндир, деб ҳисобланади. Улардан ҳимояланишнинг ягона йўли бу - программада туйнук пайдо булишига йўл қўймаслик ёки агарда программа бошқа бирор учинчи томондан қабул қилинган бўлса, дастлабки программа таҳлилларини ўтказишдан иборат.

Зарарли программалар. Сўнгги пайтларда махсус яратилган программалар ёрдамида ҳисоблаш системаларига таъсир этиш ҳоллари кўп учрамоқда. Зарарли программалар деганда информацияни ишлаш жараёнини тўғридан-тўғри ёки билвосита тўхтатиш, информацияни бузиш ва информацияни четга оқиб чиқиб кетишини таъминловчи программалар тушунилади. қуйида бундай программаларнинг энг кўп тарқалганлари билан танишиб чиқамиз. Булар: "троя тулпори", вирус, "қурт", "зиқна" программалар, "пароллар ўғриси", "бомба", "қопқон".

Мустаҳкамлаш учун саволлар:

1. Системага қасддан қилинган таъсирларни тушунтиринг.

2. система хавфсизлик сиёсатини бузувчи воситаларга нималар киради?
3. ***Зарарли программалар тушунчаси нимани англатади?***
4. ***Имтиёзлардан ноқонуний фойдаланиш тушунчасини изоҳланг.***
5. ***Рухсатсиз кириш (фойдаланиш) неча турга бўлинади ?***

Фойдаланилган адабиётлар рўйхати:

- Брассар. Ж. «Современная криптология» ,Москва, «Полимед», 1999 г.
- Петров А.А. «Криптографические методў заҳитў» ,Москва,ДМК,
-
- 2000 г.
- Романец Ю.В., Тимофеев П.А. «Заҳита информации в современнўх компьютернўх системах» , Москва, Радио и связь, 1999 г.
- Панасенко С. «Заҳита электроннўх документов» ,Москва, ФиС, 2000 г.
- Васина Е. Н., Голицина О «Информационнўе ресурсў и базў даннўх»,
- Москва, РГГУ, 1998 г.

5-6-7-**МАЪРУЗАЛАР**

Компьютер вируслари ва уларни яратишдан кўзланган мақсад. Вирус турлари ва ишлаш принциплари. AVP

умумий характеристикаси. **(6 соат)**

Ўқув модуллари

1. Компьютер вируслари.
2. Компьютер вируслари қандай пайдо бўлади?
3. Резидент ва норезидент вируслар
4. Уяли телефонлар учун вируслар.
5. Windows 98 карокчилик нусхалари билан таркаладиган вирус.
6. Антивирус программалар.
7. AntiViral Toolkit Pro антивирус программаси
8. Серверларни антивирус химоялаш.
9. Уз-узини химоялаш рецептлар

Аниқлаштирилган ўқув мақсадлари.Талаба бу мавзуни тўла ўзлаштиргандан сўнг:

- Компьютер вируслари ҳақидаги тамойилларни билади;
- Резидент ва норезидент вирусларини бўлакларга бўлиб, таъриф бера олади;
- Уяли телефонлар учун вируслар хусусиятларинини талқин эта олади;
- Windows 98 карокчилик нусхалари билан таркаладиган

Вирус қайси синфга мансублигини тасаввур эта олади;

Уз-узини химоялаш рецептлар

ўртасидаги ўзаро алоқадорликни аниқлайди, боғланишларни таҳлил қила олади.

Таянч сўз ва иборалар:

Компьютер вируслари , Резидент ва норезидент вируслари,ҳимоя моделлари, Уяли телефонлар учун вируслар , фойдаланувчи, критик информация, карок-чилик нусхалари, AntiViral Toolkit Pro антивирус программаси, Серверларни антивирус химоялаш.

Компьютер вируслари. Бу нима ва унга карши кандай курашиш керак? Бу мавзуга унлаб китоблар ва юзлаб маколалар ёзилган. Компьютер вирусла-ри-га карши минглаб профессионал мутахассислар кўплаб компанияларда иш олиб боришмокда. Бу мавзу ута қийин ва мухимки кўп эътиборни талаб килмокда. Компьютер вируси информацияни йукотиш сабабларидан бири ва асосийси

бўлиб колмокда. Вируслар кўплаб ташкилот ва компанияларни ишларини бузишга олиб келганлиги маълум. Шуи дай маълумотлар мавжудки, Нидерландия госпиталларидан бирида беморга компьютер куйган ташхис буйича истеъмол килинган дори окибатида бемор оламдан утган. Бу компьютер вирусининг иши булган.

Эътиборсизлик билан килинган ишдан компьютер тезда вирус билан зарарланади. Инсон касаллик вируси билан зарарланса иссиклиги узгариши, вазни узгариши, холсизланиш ва огрикнинг пайдо булиши кузда тутилади. Компьютер вируси билан зарарланган компьютерларда куиидагилар кузатилади: дастурларнинг ишлашининг секинлашиши, файлларци хажми узгаради, гайритабиий ва баъзи бир номаълум хатоликлар, маълумотлар ва система файллари йукотилиши. Баъзи вируслар зарарсиз кўпаяди, лекин куркинчли эмас. Бу вируслар экранга хато маълумот кикаради. Аммо, бир турдаги вируслар хужум килувчи, яъни, ёмон асоратлар колдирувчи хисобланади. Масалан, вируслар қаттиқ дискдаги информацияларни ўчирибташлайди.

Вирус нима?

Машхур «доктор» лардан бири Д.Н.Лозинский вирусни котибага ухшатади.

Тартибли котибани фараз килсак, у ишга келади ва столидаги бир кунда килиши керак булган ишларни - қоғозлар катламини куради. У бир варогни кўпайтириб бир нусхасини узига иккинчисини кейинги кушни стол га куяди. Кейинги столдаги котиба хам камида икки нусхада кўпайтириб, яна бир котибага утказади. Натижада конторадаги биринчи нусха бир неча нусхаларга айланади. Баъзи ну ехал ар яна кўпайиб бошка столларга хам утиши мумкин.

Компьютер вируслари тахминан шундай ишлайди, факат қоғозлар урнида энди дастурлар, котиба бу - компьютер. Биринчи буйруқ «кучириш-нусха олиш» булса, компьютер буни бажаради ва вирус бошка дастурларга утиб олади. Агар компьютер бирор зарарланган дастурни ишга туширса вирус бошка дастурларга таркалиб бориб бутун компьютерни эгаллаши мумкин.

Агар бир дона вируснинг кўпайишига 30 секунд вакт кетса, бир соатдан кейин бу 1000000000 дан ортиб кетиши мумкин. Аникроги компьютер хотирасидаги буш жойларни банд килиши мумкин.

Худди шундай вокеа 1988 йили Америкада содир булган. Глобал сет оркали узатилаётган информация оркали вирус бир компьютердан бошкасига утиб юрган. Бу вирус Моррис виру си деб аталган.

Маълумотларни вирус кандай йук килиши мумкин деган саволга шундай жавоб бериш мумкин:

1. Вирус нусхалари бошка дастурларга тез кўпайиб утиб олади;
2. Календар буйича 13-сана жума кунга тугри келса

ҳамма ҳужжатларни йук килади (учиради).

Буни ҳаммага маълум «Jerusalem» («Time» вируси хам деб аталади) вируси жуда «яхши» амалга оширади.

Кўп холларда билиб булмайди, вирус каердан пайдо булди.

Компьютер вируслари - кўпаювчи, дастурларни **{|Ц||га** кучиб олиши, ёмон оқибатлар келтириб чикарувчи дастурлардир. Лекин улар катъий бир куринишда булиши белгилаб куйилмаган.

Вирусни Аниқланиши шундаги, у компьютер системасида жойлашиб ва кўпайиб боришига боғлиқ. Мисол учун, назарий жихатдан оператив системада вирус даволаб булмайди. Бажарувчи коднинг сохасини тузиш ва узгартириш таъкикланган система мисол булиши мумкин.

Вирус хосил булиши учун бажарилувчи кодлар кетма-кетлиги маълум бир шароитда шаклланиши керак. Компьютер вирусининг хоссаларидан бири уз нусхаларини компьютер тармоқлари оркали бажарилувчи объектларга кучиради. Бу нусхалар хам уз-узидан кўпайиш имкониятига эга.

Компьютер вируслари кандай хосил булади?

Биологик вируслардан фаркли уларок, компьютер вирусларини инсон томонидан тузилади. Вируслар компьютер фойдаланувчиларига катта
зарар етказади. Улар компьютер ишини тухтатади ёки қаттиқ дискдаги маълумотларни учиради. Вирус системага бир неча йуллар билан тушиши мумкин: дискеталар, дастур таъминот юкланган CD-ROM, тармоқ интерфейси ёки модемли богланиш, глобал Internet тармогидаги электрон почта.

Дискета виру с дан зарарланиши осон. Зарарланган компьтерга дискетни солиб укитилганда дискнинг бош секторига вирус тушади.

Internet маълумотлар алмашинишига катта имконият яратади. Лекин, компьютер вируслари ва зарарли дастурлар таркалиши учун яхши муҳит яратади. Албатта InternetzjaH олинган барча маълумотларда вирус бор деб булмайди. Компьютерда ишловчи кўпчилик мутахассислар ва операторлар кабул килинадиган маълумотларни вируслардан текширишни доимо бажаради. Interne^a ишлаётган ҳар бир киши учун яхши антивирус химоя зарур. «Касперский лабораторияси» техник таъминот хизмати статистикасига кура, вируслардан зарарланган ҳолатларнинг 85% и электрон почта оркали содир булган. 1999 йилга нисбатан хозирги кунда бу курсаткич 70 % ташкил этади. «Касперский лабораторияси» электрон почталарга яхши антивирус химояси кераклигини таъкидлайди.

Вирус тузувчиларга электрон почта жуда кулай. Амалиёт шуни курсатадики, оммабоп дастурлар, операцион системалар, маълумотларни узатиш технологиялари учун вируслар кўплаб тузилмокда. Хозирда электрон почта бизнес ва бошка сохаларда мулокот учун асосий восита бўлиб колмокда. Шунинг учун вирус тузувчилари электрон почтага диккатини
каратмокда.

Вирус пайдо булиш белгилари.

Зарарланган компьютерда энг мухими вирусни Аниқлаш. Бунинг учун вирусни асосий белгиларини билиш керак:

1. Функционал дастурларни ишини тухтатиш ёки нотўғри ишлаши;
2. Компьютерни секин ишлаши;
3. ОС ни юкланмаслиги;
4. Файл ва каталогларни йуколиши ёки улардаги маълумотларни бузилиши;

5. Файллар модификайиясининг сана ва вактининг узгариши;
6. Файл хажмининг узгариши;
7. Дискдаги файллар микдорининг кескин кўпайиши;
8. Буш оператив хотира хажмининг кескин камайиши;
9. Кутилмаган маълумотлар ва тасвирларнинг экранга чикиши;
10.Кутилмаган товушларнинг пайдо булиши;
11 .Компьютернинг тез-тез осилиб колиши.

Юкоридаги белгилар бошка сабабларга кура хам булиши мумкинлигини эслатиб утамиз.

Кискача тарих.

80-йилларда IBM-PC билан ишлаган кишилар булса 1987-89 йиллардаги вирусларни таркалишини унутишганича йук. Экрандаги ҳарфлар ҳар хил куринишда бузилган ва фойдаланувчилар оммаси мутахассисларга дисплейларини олиб кела бошлашган. Кейинчалик компьютер «Yankee Doodle» деб номланган узга ерлик вирусини чалишни бошлаган. Лекин, буни тузатишни хеч ким ташламади, жуда тез хал булди. Бу унлаб вируслар туплами эди.

Шундай килиб, вируслар файлларни зарарлай бошлади. «Brain» ва экранда шариклар пайдо килувчи «Pingpong» вируслари Boot-сектор устидан хам голиб чикишди. Бу ҳаммаси IBM-PC дан фойдаланувчиларга унчалик ёкмади ва антивируслар пайдо булди. Биринчи антивиру ел ар дан бири ANTI-KOT: афсонавий Олег Котик узининг антивирусининг биринчи версияси дунё юзини курди. У 4 та вирусни йук килди. Афсуски, ANTI-KOT MSDOS комбинациясидан фойдаланиб файл охирида «Time» вирусини Аниқлаиди. Бошка антивируслар эса .com ва .exe кенгайтмали файлларнинг ҳар бир ҳарфигача занжирлайди.

Вакт утиши билан вируслар кўпайиб бормокда. Буларнинг ҳаммаси бир-бирига ухшаш, хотирага урнашади, сектор ва файлларга богланади, файлларни, дискет ва винчестерларни йук килади. Биринчилардан бўлиб, «Frodo.4096» вируси оммабоп бўлиб чикди. Бу вирус INT2Ih ни эгаллаб, DOS га мурожаат этилганда зарарланган файл худди хеч нарса бўлмагандай холда куриниш берган. Аммо, бу MSDOS устидан урнашиб хукмини утказган. Бир йил хам утмасданок «электр сувараклар» DOS ядросига урнашиб олишган. Куринмас вирус «Deast.512» деб аталган. Куринмаслик фикри кўпайиб ривожланиб борди: 1991 йил ёзида компьютер улати - вирус «Dir_n» пайдо булди. Бирок куринмасларга карши кураш содда: RAM ни даволаб хотиржам булиш мумкин.

Шундай вируслар хам келиб чикдики, улар узларини шифрлаб олиш имкониятига эга булишди. Бу вирусларни даволаш ва йук килиш учун махсус кием дастурлар яратиш керак булган. Лекин бунга хеч ким эътибор бермади, токи бу вирусларнинг янги авлодлари келиб чикмагунча.

Вируслар классификацияси.

Хозирги даврда 5000 дан ортик вирус дастурлар маълум. Буларни куйидагича классификацига ажратиш мумкин:

- Фаолият муҳитига караб;
- Зарарлантириш усулига караб;
- Ҳаракатланишига караб;
- Алгоритмнинг ахамиятига караб.

Фаолият муҳитидан келиб чиккан холда вирусларни сетли, файлли, юкланувчи каби турларга булинади. Сетли вируслар ҳар-хил сетли компьютерларда таркалади. Файлли вируслар бажарилувчи файлларга таркалади. Бу файллар .сом ва .exe булган файллар. Файлли вируслар бошка турдаги файлларни хам зарарлантириши мумкин. Бунда файллар бошкарувни кабул килмайди, имконият даражасини йукотади. Юкланувчи вируслар дискнинг юкловчи секторида таркалади ёки
секторнинг узида жойлашади. (Boot sektor)
Вируслар зарарлантириш усулига караб резидент ва резитент бўлмаганларга булинади. Резидент вируслар зарарланган компьютерлар оператив хотирасига узининг юкумли бир кисмини колдириб кетади. Качонки, оператив хотирага мурожаат килинганда у ишга тушади ва таркалади. Резидент вируслар компьютерни учирилгунча ва перезагрузка килингунча актив ҳолатда булади. Резидент бўлмаган вируслар компьютер хотирасини зарарлантирмайди, балки белгиланган вакт чегарасида актив ҳолатга утади.
Ҳаракатланишига караб вируслар куйидаги турларга булинади:
- Хавфсиз, компьютерда ишлашга халакит бермайди. Лекин, буш булган оператив хотира ва дискдаги хотирани камайтиради. Бундай вируслар график ва овоз эффектларида пайдо булади.
- Хавфли вируслар компьютер ишини бузишга олиб келади.
- Жуда хавфли вируслар дастурларни йукотилишига, маълумотларни ва диск системасини учиб кетишига олиб келади.

Алгоритмнинг ахамиятига караб вируслар
куйидаги группаларга булинади:
1. «Хамжихат-йулдошлар» - файлларни узгартирмайдиган вируслар. Бу вируслар EXE кенгайтмали файлларга кушимча нусха олиб, бу нусхани .сом ёки .bat кенгайтмали файл килиб ёзиб куяди. Бундай файлга мурожаат этилганда биринчи .сом ёки .bat кенгайтмали файл ишга тушади сунгра эса вирус .exe кенгайтмалисини ишга тушириб юборади.
2. "Чувалчанг-лукмалар" - бу вируслар компьютер сетларига таркайди, файл ва диск секторларини узгартирмайди. Улар компьютер сети оркали хотирага киради. Бошка вируслар адресларини топиб уларга уз нусхаларини ёзиб куяди. Бундай вируслар баъзида файллар тузади, лекин умуман компьютер ресурсларига мурожаат килмайди.
3. "Паразит" вируслар - нусхаларини диск сектори ва файлларга узгартириб таркатади. Бу вируслар юкоридагилардан фаркланади.
4. "Талаба" вируслари - жуда кўп хатоликлар келтириб чикарувчи хисобланади. Улар ҳар-хил ҳарфларни пай до килиши кутилади.
5. "Куринмас Стелс" вируси - узининг имкониятидан келиб чикиб оператив системада файлларни зарарлантириб уз урнига бошка маълумотларни куйиб "кочиб колади". Бу вируслар АВП (антивирус программалари) ни алдаб кетади.
6. "Полиморфик-ажина-мутантлар" вируси -етарлича тутиш қийин булган вируслар хисобланади. Улар Аниқ бир жойда турмайди (кучиб юради). Кўп холларда полиморфик вируслар узининг бир хил нусхасига эга булмайди.

7. "Троян отлари" вируси - керакли дастурлар ичиг-я кириб олиб ҳар бир буйруқ берилганда какшатгич зарба бера олади. У компьютер ва унинг сетлари оркали кўпайиб сезиларли зарарларни пай по ,. килади. '
8. "Макро" вируслари - асосан маълумотларн кайта ишлашга тускинлик килади ва матн муҳаррирларига зарар етказади. Хозирги вактда Microsoft Word, Excel ва Access муҳаррирларида тайёрланган ҳужжатларда кўплаб учраб туради.

Уяли телефонлар учун вируслар.

ILOVEYOU номли вирус уяли телефонлар учун мулжалланган. 2000 йилда Испанияда энг йирик Telefonika уяли алока тармогида бу вирус таркалди. Вирус мобил телефонлар учун мулжалланган бўлиб, матнли маълумотни узатади. У телефонии бузмайди, аммо алокани қийинлаштиради. Бу вирус дунё буйлаб таркалишига йул куйилмади, аммо Handheld асбоблар деб аталувчи портатив компьютерлар тармогини зарарлантирувчи янги турдаги вирусларни яратиш учун асос булиши мумкин.

Windows 98 карокчилик нусхалари билан таркаладиган вирус.

Карнеги-Меллон университета компьютер ходисаларига жавоб берувчи гурух мувофиклаштириш маркази хабарига кура 2000 йил бошида янги вирус пайдо булди. Бу Trojan.kill троян вируси бўлиб, яна -Inst98 деган номга хам эга. У С: дискдаги ҳамма маълумотларни учиради. Дастлаб у Microsoft Windows 98 операцион тизимининг крокчилик нусхаларида учради, бирок вирус электрон почта ва биргаликда фойдаланилаётган тармоқ дисклари оркали хам таркалиши мумкин. Хабар берилишича, вирус 5682 байт улчамдаги INSTALL.EXE файлида булади. Ушбу файл KEYB.COM клавиатура жойлашиш файлига кучирилади.

REMOTE EXPLORER дастури

1998 йил 17- декабрда MCI/ WorldCom ички тармоққа Remote Explorer номли вирус хужум килди. Бунинг окибатида бир канча сайтлар ва бир неча минг серверлар ва ишчи станциялар зарарланди. Вирус функциясига кура узини System 32ғdrivers га нусхасини хосил килади ва «Remote Exp1oreг»хизмати каби узини урнатади шундан сунг узини бошка машиналарга нусха куринишини бошлайди. (факатгина NT тармогида).

Вирус иш бажариш жараёнида бажарувчи файлларни зарарлаши билан биргаликда, танланган матнли файлларни хам ихтиёрий тарзда шифрлайди. Бу фаолият шанба 15:00 дан якшанба 6:00 гача булган даврда кучаяди.

Remote Explorer вируси трояплар туридаги вирусларга кушиш мумкин, чунки компьютер кайта юкланганда у йуколади ва вирус зарарланиши учун уни одатда тезда ишга тушириш керак.

«Чернобўль» вируси

1999 йил 26-апрель куни «Чернобўль» вируси туфайли дунё буйича компьютер фожиаси содир булди. Зарарланган компьютерлар хакида Англия, Швеция, Туркия, Япония, Россия, Жанубий Корея, Хиндистон, Мальта, Финлендия, Янги Зеландия ва бошка мамлакатлардан хабар келди. Евро Осиё

китъасининг мамлакатлари катта зарар курди. Умумман олганда тахминан 600000 машина ишдан чикди. Жанубий кореяда 300000 та Хитойда 100000 та, Россияда 100000 та Америкада асосан хусусий сектор, мактаблар ва университетлар (1000) зарарланди.

CIN номли вирус винчестирдаги барча маълумотларни ўчирибташлайди. У Windows 95/98 да ишлайди. Асосий таркалиш йули - электрон почта ва зарарланган дискеталар. Вирус EXE файлларга ёпишиб олади ва из колдирмайди, чунки анъанавий Аниқлаш усулларидан кочиш учун «Space Filler» хусусиятларидан яхши фойдаланади. Вирус куйидагича ишлайди: Hard drive (қаттиқ диск)нинг файл тартиби ёзиладиган соханинг маълумотнинг ўчирибюборади. Бу маълумотсиз система файлларни курмайди сунгра BIOS (Basic input Output System)га таъсир килиб, ОС ни зарарлайди. Бу эса винчестирдаги маълумотларниинг умуман учиришга олиб келади

Компьютер качон зарарланиши номаълум. Вирусни кенг таркалиши ойлаб давом этган булиши мумкин. Вирус 26-апрель куни ишга тушди. 1986 йил 26-апрель Чернобил фожеаси содир булган кун билан устма-уст тушганлиги учун

Антивирус программалар.

Компьютер вирусларидан химояланиш, уларни йук килиш ва Аниқлаш учун бир неча махсус программалар яратилган. Бундай программалар антивируслар деб аталади. Антивирус программалари турларга булинади:

- программа детекторлар;
- доктор-программалар ёки фаги;
- ревизор программалар;
- филтрловчи программалар;
- вакцина ёки иммунитет программалар.

Детектор-программалар - Аниқ вируснинг ҳарактерли ҳолатини кидиради. Оператив хотира ёки файлдаги керакли маълумотни Аниқлайди. Бундай антивирусларнинг камчилиги шундаки, улар узларига маълум булган вируснигина Аниқлайди.

Доктор-программалар ёки фаги хамда вакцина-программалар нафакат вирусларни Аниқлайди балки, даволайди, файлдаги вирус танасини учиради, файлни асл ҳолатича саклаб колади. Доктор программалар кўп микдордаги вирусларни Аниқлаш ва йук килиш имкониятига эга. Бундай программаларга: AVP, AidsTest? Scan? Norton Antivirus, Doctor Web киради.

Янги вируслар пайдо булган сари юкоридаги антивирусларнинг янги версиялари ишлаб чикиш талаб этилади.

Ревизор программалар - вируслардан ишончли химоя воситаси хисобланади. Ревизорлар дастурларни, каталоглар ва дискнинг система булими .ҳолатини компьютер вирусдан зарарланмасдан аввал эслаб колади. Шундан кейин, фойдаланувчининг хохишига биноан олдинги ва кейинги ҳолатларни солиштиради. Узгарган ҳолатларни экранга чикаради. Файлларни ҳолатини солиштиришда унинг узунлиги, модификация вакти ва санаси, хамда бошка параметрини солиштиради. Ревизор программалар етарлича мураккаб алгоритмларни хатто стелс-вирусларни хам йук килади, вирус бузиб юборган файлларни уз ҳолатига

келтиради. Бундай антивирусга кўп таркалган Россиянинг Adinf программаси мисол булади.

Фильтр-программалар ёки «тозаловчи» узида кўп бўлмаган резидент дастурларни мужассамлаштиради. Компьютернинг шубхали ва вирус характернўй берувчи ишини Аниқлайди. Бундай ҳолатларга:

1. COM ва EXE кенгайтмали файллар тартиби буйича;
2. Файл атрибутларини узгарганига караб;
3. Аниқ манзил оркали дискка ёзиш буйича;
4. Дискнинг юкловчи секторига ёзиш буйича;
5. Резидент программанинг юкланишига караб.

Бирор бир программанинг ишлаш давомида «тозаловчи» ишнинг рухсат этилиши ёки мумкин эмаслиги хакида маълумот беради. Фильтр-программалар фойдали хисобланади, у вирусни кўпайиб улгурмасидан олдин Аниқлаш имкониятини беради. Факат улар диск ва файлларни олмайди. Вирусларни йук килиш учун бошка программалар керак булади.

Вакцина ёки иммунитет программалар зарарланган файлларни даволайди. Вакциналар доктор-программалардан яхширок даволайди. Вакцина факат машхур вирусларни Аниқлайди, бунда вирус вакциналанган файл ёки дискни олиб зарарлай олмай колади. Хозирда вакциналар кам кулланилади. Зарарланган файл ва дисклардан, ҳар бир вирус тушган компьютерлардан узокрок юриш вирус эпидемиясидан сакланиш демакдир.

AntiViral Toolkit Pro антивирус программаси.

AVP фойдаланувчи учун кулай интерфейсга эга. Кўплаб кулайликларни фойдаланувчи узи белгилайди ва шу билан бирга жуда кўплаб таркалган вирусларни йук кила оладиган антивирус базасига эга.

AVP нинг иш режими куйидагича: Оператив хотира назорати. Файллар ва архивлар назорати.

Master Boot Record - система сектори, юкловчи сектор ва диск таблица назорати.

AntiViral Toolkit Pro ишининг ахамиятли томони куйидагича:

- Турли хил вирусларни йук килади, шу билан бирга уз-узини шифрловчи, куринмас ва стеле вирусларни, макро ва Word, Excel ҳужжатлари вирусларини хам йук килади.
- Упаковкаланган файлларни ичини текширади.
- Архивланган файлларни ичини текширади.
- Юмшок диск, локал, сетли ва CD-ROM дискларни текширади.
- Номаълум вирусларни текширади.
- Ортикча текшириш режими.
- Объект ичидаги узгаришларни текшириш.

AVP программаси марказий бошкарув компьютеридан автоматик равишда ишлатиш кулайдир. Бунинг учун, автоматик бошкарув буйругини тузиш талаб этилади. Баъзи бир антивирусларни кискача характеристикаси.

Dr Solomon's Antivirus Toolkit

Вирусларни Аниқлаш ва уларни йукотиш буйича энг яхши курсаткичларга эга , шунинг учун хам нархи киммат. Нархи юкорилигига карамай (85$) бу дастур «энг яхши танлов» номига сазовор булди. McAfee фирмасининг VimsScan дастури кўпрок «ёввойи» вирус-ларни учиради. Dr Solomon's Antivims Toolkit дастурининг интерфейсида ихтиёрий антивирус функциялар, барча маълум вирусларни тулик маълумоти ва уларнинг зарарлари хакида маълумотлар мавжуд. Бу дастур пакетига таркибига кирувчи юкловчи дискета Bullet («Сехрли ук») ихтимёрий системада вирусларни тез Аниқлайди ва йук килади. Бупакетнинг камчилиги хакида янги маълумотларни тармоқ оркали юклай олмаслиги хамда янги версияларни алмаштириш йилига 4 марта булади.

F-Prot Professional

Бу дастур вирусларни яхши Аниқлайди, кенг созлаш имкониятига эга, вирусларни Аниқлаганда электорн алока оркали хабар беради. Дастур камчилиги янги весриялар билан алмаштиришда паролни зарурлиги ва дастурни кайтадан урнатиш зарурлигидир. Вирусларни Аниқлаш буйича утказилган тестда 99 % вирусларни Аниқлади, лекин улардан 78 % ни учира олди. Бу дастур пакетида доимий текширувда кайси дисклар , папкалар ва файллар булиши ёки булмаслиги имкониятлари мавжуд. Бу эса вактдан ютади яъни аввал текширилган файлларни ташлаб утиши хисобига.

IBM AntiVirus v.2.5.

Вирусларни Аниқлашда катта имкониятга эга бўлиб, 1 та пакетда турли операцией системалар билан ишлаш версиялари мавжуд. Дастур камилиги вирусни учиришда консерватив (эскича) усулдан фойдаланиши. Вирусларни янги типини Аниқлашдазамонавий технологиядан фойдаланилади.Пакет нархи 49 % бўлиб, «ёввойи» вирусларни яхши Аниқлайди ва йук килади.

IBM AntiVirus вирус дастури агарда зарарланган файл вирус учиришда бузилиб кетса , у холда бу вирусни учирмайди. Бундай ҳолатда зарарланган файл умуман учирилади ва файлни резерв нусхасидан кайтадан юкланади. IBM AntiVirus дастури шундай ишлаш хисобига «ёввойи» вирусларни 32 % ни учира оладиАммо бошка дастурлар каби , IBM AntiVirus дастури юкловчи секторни заралантирувчи вирусларни 100 % учиради. Афзаллиги: янги версиялар урнатиш учун зарур файллар IBM WEB - сервер оркали олиш мумкин ва уларни урнатиш учун дастур кенг имкониятли менюга эга. Бу дастур пакетида Windows 95, 3.x , DOS ва OS / 2 системалар учун версиялар мавжуд. ENTERPRISE EDITION итшбилармонлари учун дастур пакетида Windows NT система учун версияси хам мавжуд.

Me Afee VirusScan for Windows 95

Вирусларни яхши йук килади, турли операцией системалар билан иш-лай олади, энг арзон дастур. Камчилиги: вирусларни яхши Аниқлай олмасли-ги ва янги версиялар учун кушимча хак туланиши. Me Afee VirusScan - машхур антивирус пакетларидан бири хисобланади. Утказилган тест натижаларига кура Symantec фирмасининг Norton Anti Virus дастури 13 та макровирусларни ушлади, McAfee VirusScan 12 та макровирус ушлади, 1та яъни Imposter номли кам учрайдиган

вирусни ушлай олмади. Virus Scan дастури файлли вирусларни «ёввойи» турларини қийин Аниқлайди. Текширув натжаларига кура дастур файлли вирусларни 93 % ни Аниқлади. Агарда ба дастур эффетивлиги юкори булганда эди, у яхши пакет хисобланар эди. Дастурни осон ва тез система параметрларига мослаштириб урнатиш мумкин, бунда дастур параметрларини уз ихтёрингизга кура узгартиришингиз мумкин.
Virus Scan нархи 45$ бўлиб, Windows 95, 3.x ва NT , DOS ва OS / 2 асосий операцион системалар учун версиялари мавжуд. Аммо дастурни имкониятларин кенгайтириш учун кушимча хак тулаш керак. Маълумотлар базаларини янгиланган версияларни WEB да ишлатиш мумкин, лекин McAfee WEB - сахифасига кура янги версияларни компания техник таъминотини хам олиш шарти билан ишлатиш мумкин. Кайд килинган фойдаланувчилар биринчи навбатда уч ой давомида бир марта янги версияни бепул о лиши мумкин. Шуи дан сунг 49 $ га бир йилга тузилган шартнома асосида чекланмаган микдорда дастур янги версияларни ва вирусларни янги белгиларини , хамда доимий телефон маслахатларини олиш мумкин.

Norton AntiVirus 2.0 for Windows 95

Афзаллиги вирусларни жуда яхши Аниқлайди, ажойиб интерфейс, автоматик янгиланиш. Камчилиги: «ёввойи» вирусларни 77 % ни йук килади. Бу дастур тез, ишончли ва содда мулокотли бўлиб, фойдаланувчи учун жуда кулай Мутахассислар эса узларига мослаштириб олиши мумкин.
Norton AntiVirus дастурининг интерфейсида Live Update функцияси мавжуд. Бу функция Web оркали дастурни ва вируслар белгилар тупламини янгилаши мумкин Шу билан бирга вируслар билан кураш Устаси (Virus Repair Wizard) Аниқланган вирус хакида тулик маълумот беради хамда уни йук килиш усулларни танлаш имконини беради. Бу усуллар : вирусларни автоматик равишда йук килиш ; боскичма-боскич йук килиш, бу холда учириш жараенини бошкариш мумкин.
Thunder Byte AntiVirus Utilites.
Афзаллиги: файлли вирусларни яхши Аниқлайди, текширишни жуда кулайлиги. Камчилиги: вирусларни учириши қийинрок, янги фойдаланувчилар учун учириш жараёни мураккаб. Биринчи бор Караганда, Thunder Byte AntiVirus Utilites дастури (100 $) янги вирус белгиларни Web юклаш иконiятига эга. Дастур чукуррок урганилганда, у пакетда одатдаги аъзи бир функциялар йук , аммо бир катор янги мукаммал функцияларга эга. Бу дастур Windows 95 системасининг «Проводник» дастурига ухшаш интерфейсига эга бўлиб, бошка пакетларда мавжуд бўлмаган бир катор кулайликларга эга. Текширишда сиз алохида дискларни , файлларни ёки папкаларни белгилашингиз мумкин. Thunder Byte утказилган тест натижаларига кура юкловчи сектордаги вирусларни 100% ни Аниқлайди, аммо уларни учира олмайди. Шу билан бирга дастур сикилган файлларни текширмайди, бу эса архивланган файлдаги вирусни Аниқланмаслигига олиб келади. Thunder Byte дастури компьютерда чекланган (корпоратив) ҳолатда фойдали булиши мумкин. Файлли вирусларни (макро - вируслардан ташкари) учиришдан аввал TBCLEAN номли алохида DOS утилитали дискета

хосил килиш керак. Дискетадан юкланиш, текшириш жараёнида хотирадаги вирусни фаоллашишига имкон камаяди, чунки бунда зараланган юкловчи сектор ва файлларга мурожат булмайди.

Евгений Касперский Антивирус системней.

AntiViral Toolkit Pro by Eugene Kaspersky (AVP) Microsoft кор-порациясининг тест лабораториясида сертификатланган ва "Desig-ned for Microsoft Windows95/NT", " Designed for Microsoft Win-dows 98/NT " белгиларни олган. Бу системанинг махсулотларидан бири, AVP for Windows'98? Secure Computing (АКШ ва Буюк Бри-тания) компьютер хавфсизлиги журналининг тест лабораториясида IN-the-Wild вирусларни детектирлаш буйича текширилди ва «CheckMark» белгисини олди. Бундан ташкари , AVP бошка халка-ро сертификат ва совринларга (ICSA компьютер хавфсизлиги хал-каро америка корпорацияси соврини) эга. AVP антиврус системаси таркибига бир нечта дастурлар киради:

- DOS, WINDOWS 3.XX, Windows 95/98/NT , OS/2 операцион тизимлар да ишчи станциялар учун AVP версияларидан ;
- AVP инспектори - дискни узгаришлардан химояловчи ревизор ;
- AVP for Novell Netware ва AVP for Windows NT -серверлар учун AVP версиялари ;
- Брэндмауэр (Firewall - 1) лар учун Интернетда антивирус химоя.

AVP умумий ҳарактеристикаси.

Умуман система:

- Файллардаги, юклаш секторлардаги ва оператив хотирадаги барча мавжуд турдаги файлларни излайди ва учиради ;
- «Сикилган» файлларда (PKLITE, LZEXE, DIET, COM2EXE ва бошка дастурлар форматларида) вирусларни Аниқлайди ва учиради ;
- ZIP, ARJ, LHA, RAR форматлардаги архив файлларни текширади ;
- Машхур электрон алока системалар учун локал алока кутиларни вирусга текширади;
- Эвристик механизм ёрдамида номаълум вируслар ва 32-разрядли вирусларни излайди ;
- Ностандарт заралайдиган ва файлларни бузувчи вирусларни Аниқлаш учун сканерлаш ҳолати мавжуд.

Ишчи станцияларни химоялаш.

Winfows 95, 98 , NT ва OS / 2 лар учун AVP версиялари рези-дент монитор ёрдамида фонли режимда доимий химояни таъмин-лайди.

DOS учун AVP версияси 2 вариантда мавжуд : интерфейс билан ва буйруқ сатри курининшида (AVPLITE). AVPLITE аввалги машиналарда (INTEL 286) хам ишлаши мумкин. AVPLITE - AVP туркумидаги бошка сканерлар имкониятларига эга.

AVP INSPECTOR дастури ишчи станцияларга кушимча химояни таъминлайди. Бу дискни узгаришлардан химояловчи ревизор.Дастур Windows 95/98/NT

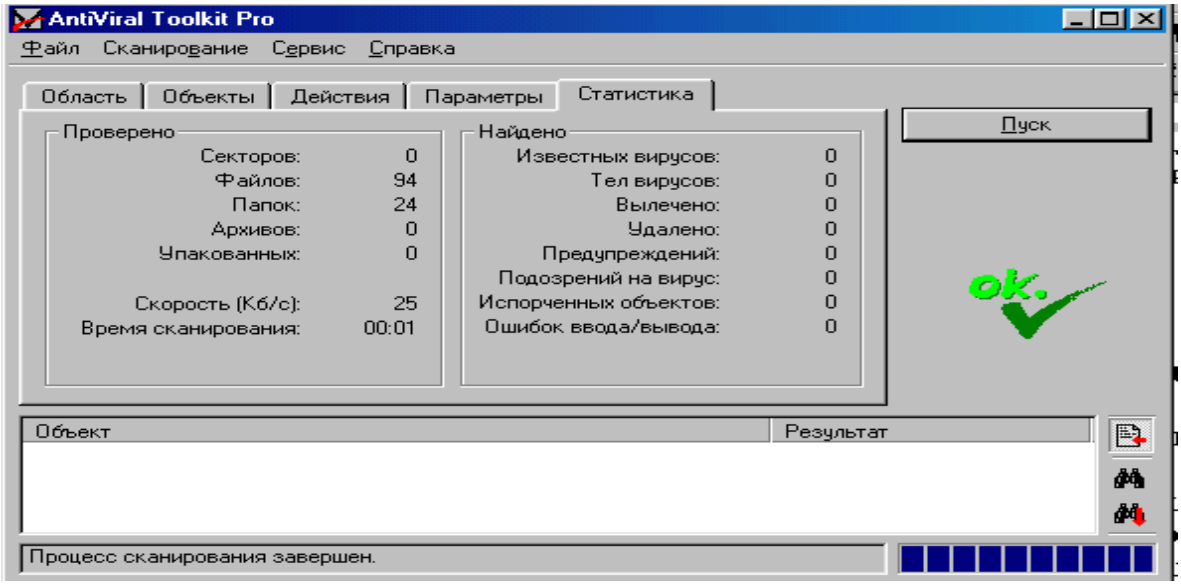
бошчилигида ишлаб, файллар ва директориялардаги, системали секторлардаги барча узгаришларни Аниқлайди.Дастур ажойиблиги, вирус хисобига ва вирус хисобига бўлмаган файлдаги узгаришини Аниқлай олиши.Масалан, AVP Inspector ёрдамида системанинг иш фаолияти (Системали реестр) боғлиқ булган ресурслардаги узгаришларни Аниқлаш мумкин. AVP Inspector сканерлаш (текшириш) вактини тежайди, чунки AVP сканери факат узгарган файлларни текширади. Бундан ташкари, дастур вирус туфайли зарарланган ва бузилган файллар ёки секторларни узи тиклаш имкониятига эга.

AVP Inspector кулай график интерфейс (GUI), кўп максадли иш юритиш, кўп окимлилик, соф 32-разрядилилик, IOS (киритиш-чикариш супервизори ёки 32-битли драйвер) драйвери оркали тугридан-тугри физик ва мантикий дискларга мурожаат килиш имкониятларига эга.

Серверларни антивирус химоялаш.

Корпоратив тармоқларга кирган вируслар кўпрок салбий таъсир утказади. Шуни хисобига, кўплаб компаниялар унлаб, баъзида юзлаб миллион дбллар йукотади.

AVPN (ёки NorellNetware учун Касперкий антивирус) - бу сканер, хам фильтр бўлиб, доимо сервердаги файлларни назорат килиб туради. AVPN сканер ҳолатида NorellNetware (3.11 версиядан бошлаб ва IntranetWare файл-серверида жойлашган) файлдаги вирусларни излайди, фильтр ҳолатида файлларни назорат килади, яъни файлларни укишда, ишга туширишда ва серверга ёзишда текширади.



AVPN зарарланган файлларни Аниқлагандан сунг уларни бошкарувчисига курсатмасига биноан, файллар дискдан ўчирибюборилиши, курсатилган жойга файлни кучириши, файл номини узгартириши мумкин. Агар да зарурат тугилса AVPN ишчи станцияни тармоқдан узиб, тармоқ администраторига хабар жунатади. AVPN нинг сканер ҳолатида битта тармоқ жойлашган узокдаги сервер томларини хам текширади.

Бундан ташкари, AVPN янги антивирус базаларини юклашга имкон беради ёки антивирус база маълумотларини AVPN дан чиқмасдан туриб тулик алмаштиришга имкон беради.

Тармоқ бошкарувчиси, AVPN билан ишлаш мобайнида унга янги созлашларни киритиши ва хотирага саклаши мумкин. Шу билан бирга ишчи станциядан дастурни ишаг тушириши ва бошкариши мумкин. AVPNHH сканер сифаьтда фойдаланилаётганда бошкарувчи уни жадвал асосида хамда ихтиёрий вакт мобайнида ишлатиши мумкин.

AVP for Windows NT Server дастури хам янги кулайликларга эга. Унинг ёрдамида система бошкарувчи тармоқдаги антивирус хавфсизлик стратегиясининг марказлашган холда бошкариши мумкин.

Бу дастур ишчи станциялардаги ва серверлардаги AVP функциясини текширишга имкон беради, хамда битта ишчи жойидан бутун тармоқ билан бошкаришга имкон беради. Хусусан, тармоқнинг барча объектларини мослаштиради. Дастур бошкарувчи тармоқнинг жорий ҳолати хакида тулик хисобот тузади ва ҳар бир ишчи станция учун автоматик янгилаш утказади.

Брэндмауэрлар учун антивирус.

Брэндмауэрлар хам химоя учун тузилади. Тармоқ рухсатсиз киришга тускинлик килгани билан доимо хам вирусларни йукота олмайди. Касперский лабораторияси, CVP (масалан, ChekPoint Fire Wall-1) протоколини таъминловчи, ихтиёрий брэндмауэрлар учун AVP for Fire Wall дастурини яратади.

AVP for Fire Wall - бу антивирус сервери бўлиб, HTTP, FTP, SMTP ва бошка протоколлар буйича кабул килинаётган файлларни текширади. Вирус Аниқланган ҳолатда, у файлни даволайди, зарарланган файл узатилиши тухтатилади, файлни алохида каталогга жойлайди ва бошкарувига алока оркали хабар беради.

<u>Уз-узини химоялаш рецептлар:</u>

! Энг яхши химоя компьютерга вирусни якинлаштирмаслик.

- умумий доимо текшириб туриш ;
- дискетга ёзиш химоясини урнатиш ;
- янги юкланган файлларни текширмасдан ишлатмаслик;
- шахсий компьютер «беркитиб» куйиш;
- доимо антивирус дастурини янгилаб бориш.

Антивирус дастурларини тест натижалари:

Антивирус дастури	Платформа	Аниқлан ган «ёв-войи» вирус-лар, %	Учирил-ган «ёв-войи» вирус-лар, %
DrSolomon's AntiVirus Toolkit	Windows 95	100	89

F - Prot Proffessional	Windows 95	99	78
IBM Anti Vims v.2.5	Windows 95	96	32
McAfee Virus Scan	Windows 95	93	90
Norton Anti Virus v. 2.0	Windows 95	100	77
Thunder Byte Antivirus Utilites	Windows 95	95	60
Touchstone PC - Cillin II	Windows 95	100	80
McAfee Virus Scan	Win-dowsNT	92	59
Norton Anti Vims v. 2.0	Win-dowsNT	100	76

"**Троя тулпори**" - бу шундай программаки, у асосан хужжатларда ёзилмаган қўшимча ҳаракатларни бажаради. қадимги Рим Троя тулпорининг аналоги бўлмиш "Троя тулпори" шубҳа ўйғотмайдиган қобиқ программаларга таъсир кўрсатиб, автоматлаштирилган система хавфсизлигига таъсир кўрсатувчи жиддий таҳдид ҳисобланади. Характерига кўра "Троя тулпори"пакет режимида ишловчи программа воситалари ёрдамида амалга ошириладиган фаол таҳдидлар турига киради. У системанинг ихтиёрий объектига тахдид солиши мумкин. Энг хавфлиси - опосредованнўй таъсир, яъни "Троя тулпори" бир фойдаланувчи ваколатлари доирасида ҳаракат қилади, лекин бошқа фойдаланувчи борасида эса унинг шахсини аниқлаш мумкин эмас.

"Троя тулпори" хавфи асосан кейинчалик система фойдаланувчиларига таклиф этиладиган (инъом этиладиган, сотиладиган ёки алмаштириладиган) зарарсиз программага у ёки бу усул билан қушилган қушимча командалар блоки-

га таъсир этишидадир. Бу командалар блоки бирор шарт (ой, йил, кун, вақт, ташқи команда) киритилганда ёки бажарилганда ишга тушади. Бундай программани ишга туширувчи ўзи ва ўзи билан бирга бутун системани ҳавф остида қолдиради.

Агар «троя тулпори»ни ишга туширган фойдаланувчи кенг имтиёзлар наборига эга бўлса, бу ҳолда унинг хавфи анча юқори бўлади. Бундай ҳолларда «троя тулпори» ни тузган ва ўзлаштирган ҳамда кенг имтиёзлар наборига эга бўлмаган бузғунчи бошқаларнинг қўли билан рухсатсиз имтиёзли функцияларни бажариши мумкин. Ёки, масалан, бундай программани ишга туширган фойдаланувчининг маълумотлар набори бузғунчини жуда қизиқтириб қолиши мумкин, бунда бузғунчининг ҳатто кенг имтиёзлар наборига эга бўлмаслиги унинг системага рухсатсиз таъсирларига тўсиқ бўла олмайди. Бунга мисол қилиб, 1999 йил январда Интернетда пайдо бўлган текин тарқатилувчи Screen saver (заставка) ни олиш мумкин, у компьютерда DES алгоритми асосидаги шифрловчи программани қилиришни амалга оширади ва агар уни топса, шифрлаш калитларининг алмашиниш жараёнини назорат қилиб, бу калитларни электрон почта орқали Хитойдаги аноним-серверга узатади. Ундан ҳимояланишнинг радикал услуби – бу программани ижро этишда берк муҳитни ташкил этишдир. Айниқса ташқи Интернет ва ички тармоқларни лоақал протоколлар сатҳида бир-биридан ажратиш (агарда бу жараён физик сатхда амалга оширилса янада яхши бўларди) лозим. Шунингдек, имтиёзли ва имтиёзсиз фойдалнувчилар турли кўринишдаги, индивидуал равишда сақланиши ва ҳимояланиши шарт бўлган программалар билан ишлагани маъқул. Бу тадбирлардан фойдаланган ҳолдагина «троя тулпори» каби программаларнинг қабул қилиниши камаяди.

Вируслар. Ҳозирда компьютер вирусига дуч келмаган бирорта ҳам система администратори ёки фойдаланувчини топиб бўлмайди. Creative Strategy Research фирмаси томонидан ўтказилган тадқиқот натижаларига кўра сўров ўтказилганда 451 мутахассисдан 64% и вирусга дуч келганини маълум қилиша-

ди. Ҳозирги кунда маълум бўлган минглаб вирусларга ҳар ойда 100-150 штаммдан келиб қўшилмоқда.

Вирус – бу шундай программаки, у бир программадан иккинчисига тез тарқала олиш хусусиятига эга бўлиб, бошқа программаларнинг таркибига ўзининг программа таркибини ўзгартирувчи хусусиятларини қўшиб қўяди. Вирусниng 2 та асосий хусусияти характерланади:

- ўзидан-ўзи кўпайиш: унинг бирор маълумот тўпловчи ёки элтувчи таркибида яшаш даврида камида битта нусхага кўпайиш хусусияти;
- ҳисоблаш жараёнига халақит бериш – тирик табиатдаги вирусларга хос паразитлик хусусияти.

Вируслар ҳам «троя тулпори» каби фаол таъсир этувчи программа бўлиб, қуйидаги 4 та қисмдан иборат структурага эга бўлади:

1-қисм – программа кодини акс эттиради, вирус унинг ёрдамида ЭҲМ хотирасига тушади;

2-қисм – вируснинг диск хотирасига, улардаги файллар ва юклаш секторига кўчирилиш ишини таъминлайди;

3-қисм – вируснинг ўз фаолиятини ишлаш шарт-шароитларини ўз ичига олади;

4-қисм – вируснинг асосий иши – бузғунчилик фаолиятини алгоритмини ўз ичига олади.

Компьютер вируслари ишлаш соҳасига қараб:

1. Компьютер системасидаги информацияни зарарловчи;
2. Компьютер системаларига инфекция юқтирувчи;
3. Компьютер системалари ва тармоқларининг ишини батамом тугатувчи турларга бўлинади.

Ҳозирги пайтда вирусларнинг синфланиши, уларда қулланиладиган вирусни юқтириш усуллари, уларга қарши курашиш чора-тадьирлари яхши ўрганилмоқда.

Вируслардан ҳимояланишда икки томондан ёндашиш мумкин:

- мустақил, алоҳида масала сифатида;

- автоматлаштирилган системанинг умумий хавфсизлигининг бир жиҳати сифатида.

Бу ёндашувларнинг иккиси ҳам ўзининг алоҳида хусусиятларига ва мос равишда масалани ечишнинг ўзига хос усулларига эга.

Вирусга қарши курашнинг бир томони сифатида Ҳозирги пайтда вирусга қарши программалар системаси ишлаб чиқилмоқда. Уларнинг кўпчилиги мос тиббий атамалар: «Вакцина», «Антитоксин», «Интерферон» ва ҳ. атамалар билан аталмоқда. Умуман олган вирусга қарши прграммаларни 3 гуруҳга ажратиш мумкин:

1. Фильтловчи программалар;
2. Вирус детекторлар (вирус ушловчилар, ревизор программалар, инфекцияга қарши программалар);
3. Фаг программалар.

Фильтрловчи программалар – заҳарланишни бартараф этиш учун ишлаб чиқилган программалар. Улар компьютер хотирасига жойлашиб олиб вирснинг уринишларини ва сигналларини кузатиб, олиб бораётган ишларини назорат қилади.

Вирус детекторлар – система ҳолатининг фото тасвирини олиб, уни доимий иш фаолияти ҳолати билан таққослаб туради. Агарда бирор ўзгариш содир бўлса, хавф тўғрисидаги сигналини беради. Бошқа ревизор программалар математик формулалар ёрдамида программа ва маълумотлар бутунлигини аниқлаб берувчи назорат кодлари йиғиндисини ҳисоблаш га асосланади.

Фаг программалар – оддий вирусларни топиб, илдизини йўқотишга ўргатилган программалар. Улар кўпроқ эски вирусларни топиб йўқотишга қулайдир.

Олиб борилган чора-тадбирлар натижасида, юқорида келтирилган программаларнинг фаолияти натижасида охирги пайтларда вируслар билан зарарланиш ва бузилиш масштабини камайтиришга эришилди. Лекин бу программаларнинг тараққиёти вирусларнинг тараққий этишига ета олмаяпти. Сўнгги йилларда компьютер вирусларидан ҳимояланишнинг истиқболли йўлларидан бири

сифатида аппарат ва программ ҳимоя усулларининг биргаликда ташкил этилишидан фойдаланилмоқда. Бундай аппарат-программ воситаларга компьютернинг стандарт кенгайтириш слотларига ўрнатиладиган махсус вирусга қарши платаларни мисол қилиш мумкин. Масалан, Intel корпорацияси 1994 йилдаёқ компьютер тармоқларини вирусдан ҳимоялашнинг истиқболли технологияси - Intel EtherExpress PRO/10 қурилмасини таклиф қилган эди. Intel EtherExpress PRO/10 қурилмаси компьютернинг бутун системасини ОС юклангунга қадар текшириб чиқувчи вирусга қарши программага ҳам эга.

«қурт» - вируслардан фарқли равишда ўз нусхасини ахборот элтувчида қолдирмайдиган, тармоқ орқали тарқалувчи программалар. «қурт» тармоқнинг бирор зарарланган узелини аниқлаш механизмидан фойдаланган ҳолда, ўзининг танаси ёки бирор қисмини ушбу узелга узатади ҳамда шу пайтнинг ўзида ишга тушади ёки бирор пайт пойлаб ишга тушади. Бундай турдаги программаларнинг энг машҳури – «Моррис қурти» бўлиб, 1988 йилда Интернет халқаро тармоғига катта зарар етказган.

«қурт»нинг тарқалиши учун энг қулай шароит бу – тармоқ фойдаланувчиларининг бир-бирига дўстона, ишонувчан муносабатларидир. Ундан ҳимояланишнинг энг яхши усули бу тармоқдан рухсатсиз фойдаланишга қарши эҳтиёт чораларини қўллашдир.

Хуллас, «троя тулпори», «қурт», вирус программалар каби зарарли программалардан ҳимояланиш учун программаларни ижро этишнинг берк муҳитини ташкил этиш, ижро этилувчи файлларга киришни чеклаш, ишлатилаётган программа воситаларини тестлаш ва ҳ. ни амалга ошириш зарур.

Мустаҳкамлаш учун саволлар:

1. ***Компьютер вируслари кандай хосил булади?***
2. *Фильтрловчи программалар қандай вазифани бажаради ?*
3. *Фаг программалар қандай вазифани бажаради ?*
4. Вируснинг қандай асосий хусусияти характерланади ?
5. ***Серверларни антивирус химоялаш тушунчасини изоҳланг.***

6. Вакцина», «Антитоксин», «Интерферон» атамалари нимани англатади ?
7. **Уз-узини химоялаш рецептларига нималар киради ?**
8. Компьютер вируслари ишлаш соҳасига қараб қандай турларга бўлинади ?
9. "Троя тулпори" хавфини изоҳланг.
10. Компьютер системаларига инфекция юқтирувчилар таркибини айтиб беринг.
11. ***Евгений Касперский Антивирус дастури имкониятларини айтиб беринг.***
12. ***Брэндмауэрлар учун антивирус нима учун тузилади ?***
13. «Моррис қурти» томонидан етказилган зарарни ифодалаб беринг.
14. *Ишчи станцияларни химоялаш* ***тушунчасини изоҳланг.***

Фойдаланилган сайтлар рўйхати

- www.securityfocus.com-портал: материалў по безопасности
- www.sans.org-Институт SANS: статьи по безопасности, проектў
- www.xforce.iss.net-база даннўх уязвимостей, материалў по безопасности
- www.packetfactory.net-сайт разработчиков библиотеке
- blacksun.box.sk/ tutorials.html-аспектам сетевой безопасности работў с сетевўх сервисов.
- www.phrack.com - журнал «Phrack»
- www.cerias.purdue.edu-Центр информационной безопасности Университет Пурду , архив программного обеспечения

8-Маъруза
Зиқна дастурлар. Маълумотларни муҳофаза қилишда шифрлаш механизмини тутган ўрни. Каналли ва абонентли шифрлаш (2 соат)

Ўқув модуллари

1. Зиқна дастурлар тушунчаси
2. Информация маҳфийлигини таъминловчи шифрлаш механизми
3. Фойдаланишни назорат қилувчи механизм .

Аниқлаштирилган ўқув мақсадлари.Талаба бу мавзуни тўла ўзлаштиргандан сўнг:

- Зиқна дастурлар ҳақидаги тамойилларни билади;
- Шифрлаш механизми асосий принципларини бўлакларга бўлиб, таъриф бера олади;
- Абонентли шифрлаш хусусиятларинини талқин эта олади;
- Рақамли имзо механизмларини қайси синфга мансублигини тасаввур эта олади;
- Маршрутни бошқариш ва гувоҳлик бериш мехинизмлари ўртасидаги ўзаро алоқадорликни аниқлайди, боғланишларни таҳлил қила олади.

Таянч сўз ва иборалар:

Зиқна дастурлар, гувоҳлик бериш механизмлари,ҳимоя моделлари,система хавфсизлиги, фойдаланувчи, каналли шифрлаш, Маршрутни бошқариш

Зиқна программалар – булар шундай программаларки, улар иш жараёнида системанинг бирор ресурсини монополлаштириб, бошқа программаларга бу ресурслардан фойдаланишга йўл қўймайди. Система ресурсларига бундай про-

граммаларнинг кириши системанинг барча ресурсларининг тенг ҳуқуқли ишлаш жараёнига путур етказади. Табиийки, бундай хужум системанинг ишига фаол таъсир этиш ҳисобланади. Бундай бевосита ҳужумларга асосан, системанинг энг муҳим объектлари – процессор, оператив хотира, киритиш-чиқариш қурилмаси, диск хотираси дучор бўлади.

Кўпчилик компьютерлар, айниқса тадқиқот марказларида фон программаларига эга бўладилар, бу фон программаларнинг эса устунлик даражаси паст бўлади. Аммо бу устунлик даражасининг ошиши натижасида программа қолган программаларни блокировка қилиб қўяди. Айнан шундай программалар зиқна программалар ҳисобланади.

Агар зиқна программа чексиз циклга тушиб қолса, система боши берк кўчага кириб қолади. Аммо кўпчилик операцион системаларда масалада фойдаланилаётган процессор вақтини чеклаш имконияти мавжуд. Бу бошқа программаларга боғлиқ боғлиқ ҳолда бажариладиган амалларга тегишли эмас, масалан, асосий программага асинхрон ҳолда бажариладиган киритиш-чиқариш амалларини келтириш мумкин; буларнинг ижро вақти программа вақти ҳисобидан ташқари бўлади. Киритиш-чиқариш амалининг тугалланганлиги тўғрисида асинхрон ахборотни олиб ва яна янги киритиш-чиқаришга сўров жўнатгандан сўнг, чин маънодаги чексиз циклли программага эришиш мумкин. Бундай хужумларни асинхрон хужумлар деб ҳам аташади.

Зиқна программаларга яна бир мисол сифатида оператив хотиранинг катта қисмини банд қилиб олувчи программани келтириш мумкин. Яъни бундай пайтда опреатив хотирада ташқи маълумот элтувчидан ўтказилган маълумотлар кетма-кет жойлаштирилади. Охир оқибатда, хотира фақат биргина программа ихтиёрида бўлиб, бошқа программалар учун оператив хотирада жой етишмаслиги натижасида, уларнинг иши тўхтайди. Юқорида айтилганидек зиқна программалар асосан ситеманинг 3 асосий ресурси: процессор вақти, оператив хотира ва киритиш-чиқариш каналларидан бирини эгаллашга ҳаракат қилади. Аммо системанинг бошқа ҳарқандай ресурсини ҳам эгаллаши мумкин: унинг ишини блокировка қилиш, ёки қандайдир программа (масалан, вирус) иш фао-

лиятининг натижаларидан фойдаланиши мумкин. Ресурсларни эгаллаб олишга қарши курашни турли ижро этилувчи программаларга чегаралар қўйиш (процессор вақти, киритиш-чиқариш амаллари сони, рухсат этилган оператив хотира сиғими ва ҳ.), шунингдек, улар устидан домий операторлик назоратини ўрнатиш йўли билан амалга оширилиши мумкин.

Пароллар ўғриси. Бу программаларни махсус ўғирлашга мўлжалланган. Системага киришга уринишда номни ва паролни киритиш сўралади ва бу парол ва ном бузғунчига жўнатилади, сўнгра киришда хатолик содир бўлгани тўғрисида ахборот чиқиб, бошқарув операцион системага қайтгандан сўнг, паролни теришда хатога йўл қўйдим деб ўйлаб фойдаланувчи системага қайтадан киришга ҳаракат қилади ва бунга муваффақ бўлади. Бу пайтда унинг номи ва парол ўғри-программанинг эгасига маълум бўлади. Паролни ўғирлаш бошқа усул – системага киришни бошқарувчи программага таъсир этиш йўли билан амалга оширилиши мумкин. Бундай таҳдидни бартараф этиш учун, аввало, киритилаётган ном ва парол ҳақикатан ҳам бошқа программа эмас, балки системанинг ҳақикий кириш программасида бажарилаётганлигига ишонч ҳосил қилиш лозим. Бундан ташқари паролдан фойдаланиш ва системада ишлаш қоидаларига оғишмай амал қилиш керак. Кўпчилик бузилишлар муғомбирлик билан қилинган пухта ўйланган таъсирлардан эмас, балки оддий бепарволик натижасида келиб чиқади. Системадан чиқиб кетмай туриб иш ўрнини тарк этмаслик тавсия этилади. Охирги марта киргандаги вақт ва кун тўғрисидаги ва хатоли киришлар сони тўғрисидаги ахборотни домий текшириб туриш зарур. Бу юқорида келтирилган барча тавсиялар паролнинг ўғирланишидан ҳимоя қилишга ёрдам беради.

Юқорида келтирилганлардан ташқари, паролни компрометация қилишнинг бошқа имкониятлари ҳам мавжуд. Паролни ўз ичига олган командаларни команда процедураларида ёзиш тавсия этилмайди, тармоққа киришдаги паролни очиқ эълон қилишдан қочиш керак, чунки бу ҳолатларни кузатиш ва натижада паролни ўғирлаш мумкин. Турли узелларга киришда битта паролдан

фойдаланмаслик керак. Хуллас, пароллардан фойдаланиш қоидаларига риоя қилиш – бу паролларни ҳимоялашнинг энг зарур шартидир.

Юқорида келтирилган қасддан қилинган таъсирлардан система ва информацияни ҳимоялаш усулларини кўриб чиқамиз.

Шифрлаш механизми узатилаётган маълумот ёки маълумотлар ҳақидаги информациянинг махфийлигини таъминлайди. Шифрлаш механизмининг алгоритмида махфий ёки очиқ калитдан фойдаланилади. Махфий калитли усулда бошқариш ва калитни тақсимлаш механизмларнинг мавжудлиги назарда тутилади. Шифрлашнинг икки усули фарқланади: канал даражасидаги протокол ёрдамида амалга оширилган ***каналли*** ва амалий даража (сатҳ) ёки баъзи ҳолларда представительний сатҳдаги протоколлар ёрдамида амалга оширилган ***абонентли (оконечное) шифрлаш***.

Каналли шифрлашда алоқа канали орқали узатилаётган барча информация (шу билан бирга хизматчи информация) ҳимоя қилинади. Бу усул қуйидаги хусусиятларга эга:

- битта канал учун шифрлаш калитини очиш бошқа каналлардаги информациянинг бузилишига олиб келмайди;
- хизматчи хабарлар, хабарларнинг хизматчи майдонини ўз ичига олган ҳолда, барча узатилаётган информация ишончли ҳимояланган;
- барча информация маълум оралиқ узеллар, ретрансляторлар, шлюзлар ва ҳ. узелларда очиқча узатилади;
- бажарилаётган операцияларда фойдаланувчи иштирок эта олмайди;
- ҳар бир жуфт узеллар учун ўзининг калити талаб қилинади;
- шифрлаш алгоритми етарли даражада маҳкам бўлиши керак ва шифрлаш суръатини каналнинг ўтказувчанлик қобилияти даражасида таъминлаши лозим (акс ҳолда хабарларнинг тутилиб қолиши рўй беради ва натижада, системанинг блокировкаси ёки ишлаш унумдорлигининг етарлича камайишига олиб келади);

- аввалги хусусият шифрлаш алгоритмини аппарат усулда амалга ошириш заруратига олиб келади, ва бунинг натижасида системанинг ташкил этилиши ва хизмат кўрсатилиши харажатларининг ошишига олиб келади;

Абонентли (оконечное) шифрлаш иккита амалий объектлар ўртасидаги узатилаётган маълумотларнинг махфийлиги ва ишончлилиги таъминлаш имкониятини беради. Бошқача айтганда, узатувчи маълумотларни шифрлайди, қабул қилувчи эса шифрланган маълумотни дешифрлайди. Бу усулнинг қуйидаги хусусиятлари бор:

- фақатгина хабарнинг мазмунигина ҳимояланади, барча хизматчи информациялар эса очиқлигича қолади;

- узатувчи ва қабул қилувчидан бошқа ҳеч ким информацияни тиклаш имкониятига эга эмас (агар фойдаланилаётган шифрлаш алгоритми етарлича мустаҳкам бўлса);

- узатиш маршрути муҳим эмас, ҳар қандай каналда информация ҳимояланган ҳолда қолади;

- ҳар бир жуфт фойдаланувчи учун ягона калит талаб қилинади;

- фойдаланувчи шифрлаш ва калитларни таққослаш процедурасини билиши керак.

У ёки бу шифрлаш усулининг ёки уларнинг комбинациясининг танланиши таваккаллар таҳлилининг натижаларига боғлиқ. Бунда савол қуйидагича қўйилади: қайси бири нозикроқ: бевосита алоҳида алоқа каналими ёки турли каналлар орқали узатилаётган хабарнинг мазмуними? Канални шифрлар тезроқ (бошқа бундан ҳам тезроқ алгоритмларни қўллаш мумкин), фойдаланувчи учун равшан, камроқ калитларни талаб қилади. Абонентли шифрлаш нисбатан ихчамроқ, сайланма тарзда фойдаланилиши мумкин, бироқ бунда фойдаланувчининг иштирок этиши талаб қилинади. Ҳар қандай аниқ бир шароитда бу масала индивидуал равишда ечилади.

Рақамли имзо механизмлари – маълумотлар блокини ёпиш ва ёпилган маълумотлар блокини текшириш процедураларига эга. Дастлабки жараён

махфий калитли маълумотларни тиклашга йўл қўймайдиган очиқ информациядан фойдаланади. Махфий информация ёрдамида жўнатувчи хизматчи маълумотлар блокини шакллантиради (масалан, бир томонлама функция ёрдамида) қабул қилувчи эса ҳамманинг фойдаланиши мумкин бўлган информация асосида қабул қилинган блокни текширади ва жўнатувчининг ҳақиқий (асл, чин) эканлигини аниқлайди. Асл маълумотлар блокини фақат зарур калитни биладиган фойдаланувчигина шакллантира олиши мумкин.

Фойдаланишни назорат қилиш механизми – тармоқ объектининг ресурсларидан фойдаланиш учун қанчалик ваколатларга эгалигини текширади. Ваколатларни текшириш ишлаб чиқилган хавфсизлик сиёсати (сайлов, ваколатли ёки ихтиёрий бошқа) ва уни амалга ошириш механизмларининг қонун-қоидаларига мувофиқ ҳолда амалга оширилади.

Узатилаётган маълумотларнинг бутунлигини таъминлаш механизмлари – бу механизмлар маълумотларнинг алоҳида майдони ёки блокининг бутунлигини қандай таъминласа, тўла маълумотлар оқимининг бутунлигини ҳам шундай таъминлайди. Маълумотлар блокининг бутунлиги узатувчи ва қабул қилувчи объектлар томонидан таъминланади. Узатувчи объект маълумотлар блокига шундай қўшимча белги қўшадикик, бу белги шу маълумотларнинг ўзидан ҳосил қилинган функциянинг қийматига тенг бўлади. қабул қилувчи объект ҳам худди ҳосил қилинган функцияни ҳисоблайди ва уни қабул қилинган маълумот билан таққослайди. Агар бу ерда улар бир-бири билан мос келмаса, маълумотларнинг бутунлиги бузилганлиги маълум бўлади. Маълумотда ўзгаришни пайқагандан кейин маълумотларни тиклаш ишлари олиб борилади.

Маълумотларнинг бутунлигини қасддан бузишда мос равишда назорат белгисининг қиймати ҳам ўзгартирилиши мумкин, бундай пайтларда қабул қилувчи маълумотлар бутунлигининг бузилганлигини пайқамайди. Шунинг учун бундай шароитда назорат белгисини маълумотларнинг ва махфий калитнинг функцияси кўринишида шакллантириш керак. Бундай ҳолда назорат бел-

гисини махфий калитни билвосита туриб тўғри шакллантириб бўлмайди ва қабул қилувчи бу ўзгартириш натижасида асл маълумотми ёки йўқлиги тўғрисида аниқ хулосага келади.

Маълумотлар оқимининг бутунлигини (қайта ўзгартиришдан, қўшимча маълумот қўшишдан, маълумотларнинг такрорланишидан ёки йўқолишидан) ҳимоя қилишни қўшимча тартиблаш шакллари (маълумотлар оқимидаги хабарларнинг тартибини назорат қилиш), вақт белгилари ва ҳ.дан фойдаланиб амалга ошириш мумкин.

Тармоқ объектларининг аутентификацияси механизмлари – аутентификацияни таъминлашда пароллар, объект характеристикаларини текшириш, криптографик методлардан, рақамли имзо кабилардан фойдаланилади. Бу механизмлар одатда, бир сатҳли тармоқ объектларини аутентификация қилишда фойдаланилади. Фойдаланилаётган усуллар “уч карра қўлни қисиш” процедураси билан бир вақтда олиб борилиши мумкин (жўнатувчи ва қабул қилувчи ўртасида аутентификация ва тасдиқлаш параметрлари билан ахборот алмашиш уч карра амалга оширилиши).

Матнни тўлдириш механизмлари – графикни анализ қилишдан ҳимояни таъминлаш учун ишлатилади. Бундай механизм сифатида, масалан, (фиктив) сохта ахборотни генерация қилишдан фойдаланиш мумкин, бунда трафик вақт бўйича доимий интенсивликка эга.

Маршрутни бошқариш механизмлари – маршрутлар динамик танланиши мумкин ёки физик хавфсиз қисм тармоқ, ретрансляторлар, каналлардан фойдаланган ҳолда олдиндан берилиши мумкин. Чирмаб боғлашга уринишда тугал (абонент) системалар бошқа маршрут бўйича боғланишни талаб қилади. Бундан ташқари, танлов бўйича маршрутлашдан фойдаланилиши мумкин (яъни маршрутнинг бир қисми жўнатувчи томонидан очиқ ҳолда хавфли участкаларни айланиб чиқишда берилади).

Гувоҳлик бериш механизмлари – икки ёки ундан ортиқ объектлар ўртасида узатилаётган маълумотларнинг характеристикалари ***гувоҳлик бериш механизми*** орқали тасдиқланиши мумкин. Тасдиқлаш барча томонларнинг ишончига сазовор бўлган учинчи томон - арбитр томонидан амалга оширилади.

Ҳодисаларни топиш ва ишлаш (хавфли ҳодисларни назорат қилиш воситалари каби) – тармоқнинг хавфсизлик сиёсатининг бузилишига олиб келувчи ҳодисаларни топишга мўлжалланган. Бу ҳодисаларнинг рўйхати алоҳида системалардаги рўйхатга мувофиқ келади. Бундан ташқари, бунга юқорида келтирилган ҳимоя механизмларининг ишидаги бузилишлар тўғрисида маълумот берувчи ҳодисаларни ҳам киритиш мумкин. Бундай ҳолларда кўриладиган чора-тадбирларга турли процедуралар: тиклаш, ҳодисаларни рўйхатга олиш, алоқани бир томонлама узиш, ҳодиса ҳақида ҳисобот (журналга ёзиш) ва ҳ. процедураларни киритиш мумкин.

Хавфсизликни текшириш ҳисоботи (система журнали билан текшириш каби) – хавфсизликни текшириш деганда система ёзувлари ва фаолиятининг берилган хавфсизлик сиёсатига мослигини мустақил текшириш тушунилади.

Мустаҳкамлаш учун саволлар:

1. ***Гувоҳлик бериш механизмлари нимани англатади ?***
2. хавфсизликни текшириш деганда *нима тушунилади ?*
3. ***Маршрутни бошқариш механизмлари***
4. Вируснинг қандай асосий хусусияти характерланади ?
5. ***Серверларни антивирус химоялаш тушунчасини изоҳланг.***
6. ***Узатилаётган маълумотларнинг бутунлигини таъминлаш механизмлари***
   Деганда нима тушунилади?
7. **Уз-узини химоялаш рецептларига нималар киради ?**
8. Компьютер вируслари ишлаш соҳасига қараб қандай турларга бўлинади ?

Фойдаланилган сайтлар рўйхати

- www.xforce.iss.net-база даннўх уязвимостей, материалў по безопасности
- www.packetfactory.net-сайт разработчиков библиотеке
- blacksun.box.sk/ tutorials.html-аспектам сетевой безопасности работў с сетевўх сервисов.
- www.phrack.com - журнал «Phrack»
- www.cerias.purdue.edu-Центр информационной безопасности Университет Пурду , архив программного обеспечения

9-МАЪРУЗА

Локал ҳисоблаш тармоқларида маълумотларни муҳофаза қилиш усули (2 соат)

Ўқув модуллари

1. Информацияни ҳимоялашнинг асосий усуллари
2. **Идентификация ва аутентификация тушунчалари**
3. ***Статик аутентификация***
4. ***Ўзгармас аутентификация***

Аниқлаштирилган ўқув мақсадлари.Талаба бу мавзуни тўла ўзлаштиргандан сўнг:

- Информацияни ҳимоялашнинг асосий усуллари ҳақидаги тамойилларни билади;
- **Идентификация ва аутентификация тушунчалари** асосий принципларини бўлакларга бўлиб, таъриф бера олади;
- ЛҲТ нинг баъзи объектлари ва ресурсларидан фойдаланиш хусусиятларинини талқин эта олади;
- ***Барқарор аутентификация*** қайси синфга мансублигини тасаввур эта олади;
- Аутентификациянинг учта асосий кўриниши ўртасидаги ўзаро алоқадорликни аниқлайди, боғланишларни таҳлил қила олади.

Таянч сўз ва иборалар:

Идентификация , аутентификация, Информацияни ҳимоялаш, ЛҲТ, ***Барқарор аутентификация, Статик аутентификация, Ўзгармас аутентификация,*** серверлар диски (томи),, ишчи станция, каталог **.**

Информацияни ҳимоялашнинг асосий усулларига қуйидагилар киради:

- ЛҲТ га киришда аутентификация ва идентификация қилиш;

- ЛҲТ нинг баъзи объектлари ва ресурсларидан фойдаланишни чеклаш (алоҳида серверга, алоҳида серверлар диски (томи) га, ишчи станция, каталог, файллардан фойдаланиш, уларни ўзгартириш, ўчириш ва ҳ.к.).

- ЛҲТ да информацияни ҳимоя қилишнинг аппарат усули.

- Маълумотларни ҳимоя қилишнинг программа усули;

- Маълумотларни криптографик усулда ҳимоя қилиш, яъни маълумотларни шифрлаш (криптлаш);

1. Идентификация ва аутентификация

Идентификация ва аутентификация (Ид ва А) - фойдаланувчи ва жараёнлар тўғрисидаги маълумотларнинг ҳақиқийлигини (асллигини) текшириш ва аниқлаш жараёнидир. Улар фойдаланувчига система ресурсларидан фойдаланишининг мумкин ёки мумкин эмаслиги ҳақида қарор қабул қилишда ишлатилади. У ёки бу маълумотдан кимлар фойдалана олиши мумкинлигини аниқлаш маълумотлар синфланиши жараёнининг таркибий қисми бўлиши лозим.

Аутентификациянинг учта асосий кўриниши мавжуд бўлиб, улар - статик, барқарор ва ўзгармас. Статик аутентификация пароллардан ва бошқа технологиялардан фойдаланади. Бу парол ва технологияларни такрорлаш йўли билан йўққа чиқариш мумкин. Одатда, бу пароллар такрор фойдаланиладиган деб номланади. Барқарор аутентификация бир марта ишлатиладиган паролларни яратиш учун криптографиядан фойдаланади. Бу усул тармоққа уланиш жойига атака қилувчи хабарларни қўйиш билан йўққа чиқарилади. Ўзгармас аутентификация тармоққа уланиш жойига атака қилувчи информацияни қўйишдан сақлайди.

Статик аутентификация

Статик аутентификация аутентификацияловчи ва аутентификацияланувчи томонлар ўртасида узатилаётган информацияни ёт ҳужум қилувчи томон кўра

олмайдиган, ўзгартира олмайдиган, қўя олмайдиган пайтдагина ҳимояни таъминлайди. Бундай ҳолатда бузғунчи фақат аутентификация жараёнини бошлаш (буни фақат қонуний фойдаланувчи амалга ошира олади) ва бир қатор уринишларни амалга ошириш ёрдамидагина маълумотларни аниқлашга уриниши мумкин. Пароллардан фойдаланишнинг анъанавий схемалари ҳимоянинг мана шу туридан фойдаланади. Лекин аутентификация мустаҳкамлиги асосан паролларни топишнинг мураккаблиги ҳамда бу паролларнинг қанчалик даражада яхши ҳимояланганлигига боғлиқ бўлади.

Барқарор аутентификация

Аутентификациянинг бу синфи ҳар бир аутентификация сеансларида алмашиниб турадиган динамик аутентификация маълумотларидан фойдаланади. Аутентификацияловчи ва аутентификацияланувчи орасида узатиладиган информацияни тутиб қолиши мумкин бўлган атака қилувчи янги аутентификация сеансини аутентификацияланувчи билан биргаликда бошлашга ва қонуний фойдаланувчи назорати остида ниқоблаш умидида маълумотларни такрорлашга ҳаракат қилади. 1-даражали кучайтирилган аутентификация шундай атакалардан ҳимоя қиладики, бу атака натижасида олдинги сеансда ёзилган аутентификация маълумотларидан кейинги сеансларда фойдаланиш мумкин бўлмай қолади.

Шунга қарамасдан, барқарор аутентификация маълумотларни фаол атакалардан ҳимоя қила олмайди. Бундай атакалар аутентификация жараёни тугагандан сўнг фойдаланувчи томонидан серверга жўнатиладиган команда ва маълумотлар атака қилувчи томонидан ўзгартирилиши натижасида амалга оширилади. Сервер берилган аутентификацияланаётган фойдаланувчи ва мантиқий уланиш ўртасидаги алоқани таъминлайди; у ўзини ушбу уланишга тааллуқли барча командаларнинг манбаи деб ҳисоблайди..

Анъанавий пароллар барқарор аутентификацияни таъминлай олмайди. Фойдаланувчи пароллари кейинчалик фойдаланилиши ёки тутиб қолиниши

мумкин. Лекин бир марталик пароллар ва электрон имзолар ушбу ҳимоя даражасини таъминлай олади.

Ўзгармас аутентификация

Аутентификациянинг бу тури аутентификацияланувчи ва аутентификацияловчи орасида узатиладиган маълумотлар оқими орасига информация қўшиши, ўзгартириши ва тутиб қолиши мумкин бўлган атака қилувчидан ҳаттоки, аутентификация жараёни тугагандан сўнг ҳам ҳимояни таъминлайди. Бундай атакалар фаол атака деб юритилиб, атака қилувчи, асосан, сервер ва фойдаланувчи орасидаги боғланишга фаол таъсир кўрсатади. Ҳимоянинг бу турини амалга оширишнинг усулларидан бири фойдаланувчидан серверга жўнатилаётган ҳар бир маълумотлар битига ишлов беришни электрон имзоларни инерция қилиш алгоритми ёрдамида амалга оширишдан иборат. Криптография асосидаги бошқа комбинациялар ҳам мавжудки, булар ёрдамида аутентификацияни амалга ошириш мумкин. Лекин, мавжуд стратегияларда ҳар бир маълумот битини ишлаш учун шифрлашдан фойдаланилади. Акс ҳолда маълумотлар оқимининг ҳимоя қилинмаган қисми шубҳали ҳолда қолиши мумкин.

Тармоққа киришда ва фойдаланувчи номини киритишда идентификация, парол киритишда аутентификация амалга оширилади. Агарда фойдаланувчи ушбу парол ва ном билан системада қайд қилинган бўлса, унга аниқ объект ва ресурслардан фойдаланишга рухсат этилади. Бироқ системага киришда, бу функцияларнинг бажарилиш жараёнида баъзи фарқлар мавжуд. Бу фарқлар иш жараёнида система ким ишлаётгани, унинг қандай ҳуқуқлари борлиги ва ҳоказолар ҳақида информацияга эга эканлигига асосланади ва шунинг учун мос ҳолда субъект саволларига жавоб қайтаради. Системага киришда буларнинг ҳаммасини олдиндан аниқлаш керак бўлади. Ушбу ҳолатда аслликни таъминлаш мақсадида фойдаланувчидан хавфсизлик ядроси томон боришда идентификацияловчи информациянинг узатилиш йўли - “ишончли маршрут”ни ташкил этиш зарурияти туғилади. Амалиёт шуни кўрсатадики, фойдаланувчининг системага кириши - ҳимоянинг анчагина нозик жойларидан биридир: кўпчилик

ҳолларда паролларни синдириш, паролсиз кириш, паролларни тутиб қолиш ва ҳоказо ҳолатлар рўй беради. Шунинг учун фойдаланувчи ҳам, система ҳам ўзаро бевосита ишлаётгани, улар орасида бошқа программа ёки узатилувчи информациялар йўқлиги ҳақида ишонч ҳосил қилиши керак.

Фойдаланувчи идентификаторлари ва уларнинг пароллари ҳар бир фойдаланувчи учун ягона бўлиши керак.

Пароллар 6 та символдан кам бўлмаслиги ва машҳур номлар ёки иборалардан тузилмаслиги лозим. Ўйлаб топиладиган паролларнинг пайдо бўлишини доимий равишда махсус программалар ёрдамида текшириб туриш зарур. Бундай программаларда ўйлаб топиладиган пароллар генерацияси бўйича қоидалар тўплами бўлиши лозим.

Пароллар махфий ҳолда сақланиши, яъни бошқа одамларга айтилмаслиги, программа матнида ва ҳар хил қоғозларда ёзилмаслиги ҳамда ҳар 90 кунда алмаштирилиши лозим. Кўпчилик системалар маълум вақт ўтгач паролни мажбурий алмаштириши ва аввал фойдаланилаётган паролни йўққа чиқариши мумкин.

Фойдаланувчилар бюджети системага киришда 3 та муваффақиятсиз уринишдан сўнг “қотиб қолиши” ҳамда нотўғри киритилган пароллар номи система журналига киритиб қўйилиши керак.

Фойдаланувчи ва сервер орасида бўладиган иш сеанси 15 минут давомидаги фаолиятсизликдан сўнг блокировка қилиниши лозим. Сеанс ишини қайта тиклаш учун яна парол киритиш талаб қилиниши керак.

Системага муваффақиятли кирилганда, ундан охирги марта фойдаланилган сана ва вақт акс эттирилиши лозим.

Фойдаланувчилар бюджети маълум вақт фойдаланилмагандан сўнг блокировка қилиниши шарт.

Юқори таваккалли системалар учун: бир қанча берухсат кириш учун уриниб кўришлардан сўнг система огоҳлантириш сигналини бериши ва бу уринишларни амалга ошираётган фойдаланувчи учун сервернинг ёлғон хабарларини бериши лозим.

Чунки у системага қўшилган ҳолда турган вақтда хавфсизлик администратори унинг жойлашган ўрнини аниқлашга ҳаракат қилади.

Мустаҳкамлаш учун саволлар:

1. ***Ўзгармас аутентификация нимани англатади ?***
2. Аутентификациянинг учта асосий кўриниши деганда *нима тушунилади ?*
3. ***Маршрутни бошқариш механизмлари тушунчасини изоҳланг.***
4. Информацияни ҳимоялашнинг асосий усулларига нималар киради ?
5. ***Серверларни антивирус химоялаш тушунчасини изоҳланг.***
6. ***Узатилаётган маълумотларнинг бутунлигини таъминлаш механизмлари***
7. Анъанавий пароллар барқарор аутентификацияни таъминлай оладими ?

Фойдаланилган адабиётлар рўйхати:

- Брассар. Ж. «Современная криптология» ,Москва, «Полимед», 1999 г.
- Петров А.А. «Криптографические методў заҳитў» ,Москва,ДМК, 2000 г.
- Романец Ю.В., Тимофеев П.А. «Заҳита информации в современнўх компьютернўх системах» , Москва, Радио и связь, 1999 г.
- Панасенко С. «Заҳита электроннўх документов» ,Москва, ФиС, 2000 г.
- Васина Е. Н., Голицина О «Информационнўе ресурсў и базў даннўх», Москва, РГГУ, 1998 г.
- Попов И.И. «Автоматизированнўе информационнўе системў» , Москва, РГГУ, 1998 г.
- Митчелл Ш. «Тольковўй словарь компьютернўх технологии», Москва,2000г

АХБОРОТ КЎРСАТКИЧИ

1. Маълумотларни муҳофаза қилиш тушунчаси.Муҳофаза системаси
2. Тасодифий таъсирлар ва улардан информацияни муҳофаза қилиш усуллари.
3. қасддан қилинган таъсирларнинг турлари ҳамда улардан маълумотларни муҳофаза қилиш усуллари

II. ЛОКАЛ ҲИСОБЛАШ ТАРМОҚЛАРИДА ИНФОРМАЦИЯНИ ҲИМОЯЛАШНИНГ УСУЛЛАРИ

1. **Идентификация ва аутентификация.**
2. **ЛҲТ нинг алоҳида ресурсларидан фойдаланишнинг чегараланиши**
3. **ЛҲТ ҳимоясининг аппарат усуллари**
4. **Маълумотларни ҳимоя қилишнинг программа усули**
5. **Операцион системани ҳимоя қилиш воситалари**
6. **Тармоқ мониторинги воситалари**
7. **Информацияни криптографик ҳимоя қилиш воситалари**

Фойдаланилган адабиётлар рўйхати

4. С.Петренко ,М.Мамаев «Технологии заҳитў в Интернете» Издательский дом «Питер» , Санкт-Петербург, 2002 г.
5. Турский А. , Панов С «Заҳита информации при взаимодействии корпоратив-нўх сетей в Интернет» , ФиС, Москва, 2003 г.
6. Кошелев А.»Заҳита сетей и firewall» КомпьютерПресс, 2000 г.
7. Оливер .В.Г. «Новўе технологии и оборудование» ,СПб:BHV-Санкт – Петербург,2000 г.
8. Брассар. Ж. «Современная криптология» ,Москва, «Полимед», 1999 г.
9. Петров А.А. «Криптографические методў заҳитў» ,Москва,ДМК, 2000 г.
10. Романец Ю.В., Тимофеев П.А. «Заҳита информации в современнўх компью-тернўх системах» , Москва, Радио и связь, 1999 г.
11. Панасенко С. «Заҳита электроннўх документов» ,Москва, ФиС, 2000 г.
12. Васина Е. Н., Голицина О «Информационнўе ресурсў и базў даннўх», Москва, РГГУ, 1998 г.
13. Попов И.И. «Автоматизированнўе информационнўе системў» , Москва, РГГУ, 1998 г.
14. Митчелл Ш. «Тольковўй словарь компьютернўх технологии», Москва,2000г

Фойдаланилган сайтлар рўйхати

- www.securityfocus.com-портал: материалў по безопасности
- www.sans.org-Институт SANS: статьи по безопасности, проектў
- www.xforce.iss.net-база даннўх уязвимостей, материалў по безопасности
- www.packetfactory.net-сайт разработчиков библиотеке
- blacksun.box.sk/ tutorials.html-аспектам сетевой безопасности работў с сетевўх сервисов.
- www.phrack.com - журнал «Phrack»
- www.cerias.purdue.edu-Центр информационной безопасности Университет Пурду , архив программного обеспечения

Русскоязўчнўе ресурсў:

- www.void.ru
- www.hackzone.ru
- www.security.nnov.ru
- www.xaker.ru