LECTURE-9: CYBER SECURITY

МАЪРУЗА -9: КИБЕРХАВФСИЗЛИК

Ахборот хавфсизлиги деб, маълумотларни йўқотиш ва ўзгартиришга йўналтирилган табиий ёки сунъий хоссали тасодифий ва қасддан таъсирлардан хар қандай ташувчиларда ахборотнинг ҳимояланганлигига айтилади.

Ахборотнинг ҳимояси деб, бошқариш ва ишлаб чиқариш фаолиятининг ахборот хавфсизлигини таъминловчи ва ташкилот ахборот захираларининг яхлитлилиги, ишончлилиги, фойдаланиш осонлиги ва махфийлигини таъминловчи қатьий регламентланган динамик технологик жараёнга айтилади.

Киберхавфсизлик ҳозирда кириб келган янги тушунчалардан бири бўлиб, унгатурли берилган турли таърифлар мавжуд.

Хусусан, киберхавфсизликка қуйидагича таъриф берган: киберхавфсизлик - ҳисоблашга асосланган билим соҳаси бўлиб, бузгунчилар мавжуд бўлган шароитда амалларни кафолатлаш учун ўзида технология, инсон, ахборот ва жараённи мужассамлаштирган.

У хавфсиз компьютер тизимларини яратиш, амалга ошириш, таҳлил қилиш ва тестлашни ўз ичига олади.

Киберхавфсизлик таълимнинг мужассамлашган билим соҳаси бўлиб, қонуний жихатларни, сиёсатни, инсон омилини, этика ва рискларни бошқаришни ўз ичига олади.

Тармоқ бўйича фаолият юритаётган киберхавфсизликка қуйидагича таъриф берилган: Киберхавфсизлик - тизимларни, тармоқларни ва дастурларни рақамли ҳужумлардан ҳимоялаш амалиёти.

Ушбу киберҳужумлар одатда махфий ахборотни бошқариш, алмаштириш ёки йўқ қилишни; фойдаланувчилардан пул ундиришни; ёки нормал иш фаолиятини узуб қўйишни мақсад қилади.

• Ҳозирги кунда самарали киберхавфсизлик чораларини амалга ошириш инсонларга қараганда қурилмалар сонининг кўплиги ва бузгунчилар салоҳиятини ортиши натижасида амалий томондан мураккаблашиб бормоқда.

Киберхавфсизликни фундаментал терминларини қараб чиқамиз:

Конфиденциаллик

Тизим маълумоти ва ахборотига фақат ваколатга эга субъектлар фойдаланиши мумкинлигини таъминловчи қоидалар.

Мазкур қоидалар ахборотни фақат қонуний фойдаланувчилар томонидан “ўқилишини” таъминлайди.

Яхлитлик (бутунлик)

Маълумотни аниқ ва ишончли эканлигига ишонч ҳосил қилиш.

Яъни, ахборотни рухсат этилмаган ўзгартиришдан ёки “ёзиш” дан ҳимоялаш.

Фойдаланувчанлик

Маълумот, ахборот ва тизимдан фойдаланишнинг мумкинлиги.

Яъни, рухсат этилмаган “бажариш” дан ҳимоялаш.

“Маьлумотлар хавфсизлиги” билим соҳаси маьлумотларни еақлашда, қайта ишлашда ва узатишда ҳимояни таъминлашни мақсад қилади.

Мазкур билим соҳаси ҳимояни тўлиқ амалга отттириттт учун математик ва аналитик алгоритмлардан фойдаланишни талаб этади.

“Даетурий таьминотлар хавфеизлиги” билим соҳаси фойдаланилаётган тизим ёки ахборот хавфсизлигини таъминловчи даетурий таьминотларни ишлаб чиқиш ва фойдаланиш жараёнига эътибор қаратади.

“Ташкил этувчилар хавфеизлиги” билим соҳаси катта тизимларда интеграллашган ташкил этувчиларни лойиҳалаш, еотиб олиш, теетлаш, анализ қилиш ва техник хизмат кўрсатишга эътибор қаратади.

Тизим хавфсизлиги ташкил этувчилар хавфсизлигидан фарқ қилади.

Ташкил этувчилар хавфсизлиги улар қандай лойиҳаланганлиги, яратилганлиги, сотиб олинганлиги, бошқа таркибий қисмларга уланганлиги, қандай ишлатилганлиги ва сақланганлигига боғлиқ.

“Алоқа хавфеизлиги” билим соҳаси ташкил этувчилар ўртасидаги алоқани ҳимоялашга этибор қаратиб, ўзида физик ва мантиқий уланишни бирлаштиради.

“Тизим хавфсизлиги” билим соҳаси ташкил этувчилар, уланишлар ва даетурий таьминотдан иборат бўлган тизим хавфсизлигининг жиҳатларига эътибор қаратади.

Тизим хавфсизлигини тушуниш учун нафақат, унинг таркибий қисмлари ва уланишини тушунишни, балки бутунликни ҳисобга олишни талаб қилади.

“Инсон хавфсизлиги” билим соҳаси киберхавфсизлик билан боглиц инсон ҳатти ҳаракатларини ўрганишдан ташқари, ташкилотлар (масалан, ходим) ва шахсий ҳаёт шароитида шахсий маълумотларни ва шахсий ҳаётни ҳимоя қилишга эътибор қаратади.

“Ташкилот хавфсизлиги” билим соҳаси ташкилотни киберхавфсизлик таҳдидларидан ҳимоялаш ва ташкилот вазифасини муваффацциятли бажаришини мададлаш учун рискларни бошқаришга эътибор қаратади.

Киберхавфсизлик сиёсати бу - ташкилотнинг мақсади ва вазифаси ҳамда хавфсизликни таъминлаш соҳасидаги чора-тадбирлар тавсифланадиган юқори сатҳли режа ҳисобланади.

У хавфсизликни таъминлашнинг барча дастурларини режалаштиради.

Ахборот хавфсизлиги сиёсати ташкилот масалаларини ечиш ҳимоясини ёки иш жараёни ҳимоясини таъминлаши шарт.

Аппарат воситалар ва дастурий таъминот иш жараёнини таъминловчи воситалар ҳисобланади ва улар хавфсизлик сиёсати томонидан қамраб олиниши шарт.

Ташкилотнинг амалий хавфсизлик сиёсати қўйидаги бўлимларни ўз ичига олиши мумкин:

умумий низом;

паролларни бошқариш сиёсати;

фойдаланувчиларни идентификациялаш;

фойдаланувчиларнинг ваколатлари;

ташкилот ахборот коммуникацион тизимини компьютер вируслардан ҳимоялаш;

тармоқ уланишларини ўрнатиш ва назоратлаш қоидалари;

электрон почта тизими билан ишлаш бўйича хавфсизлик сиёсати қоидалари;

ахборот коммуникацион тизимлар хавфсизлигини таъминлаш қоидалари;

фойдаланувчиларнинг хавфсизлик сиёсатини қоидаларини бажариш бўйича мажбуриятлари ва ҳ.к.лар

Киберхавфсизлик рискларини аниқлашнинг умумий тавсифини қраб чиқамиз. РИСК номақбул воқеа - ҳодисадан келиб чиқадиган оқибатлар ва воқеа- ҳодиса юзага келиши эҳтимоллиги бирикмасини ўзида ифодалайди. Рискларни аниқлаш миқдор ёки сифат жиҳатдан рискларни тавсифлайди ва раҳбарларга қабул қилинадиган жиддийликка ёки бошқа ўрнатилган мезонларга кўра устуворликларга мувофиқ рискларни жойлаштириш имкониятини беради.

Рискни аниқлаш қуйидаги тадбирлардан иборат:

- рискларни аниқлаш;
- рискларни идентификация қилиш;
- рискларни таҳлил қилиш;
- рискларни баҳолаш.

Рискларни аниқлаш ахборот активларининг аҳамиятини белгилайди, мавжуд (ЁКИ мавжуд бўлиши мумкин) қўлланиладиган таҳдидлар ва заифликларни идентификация қилади, мавжуд бошқариш воситаларини ва уларнинг идентификация қилинган рискларга таъсирини идентификация қилади, потенциал оқибатларни аниқлайди ва НИҲОЯТ, устуворликларга мувофиқ, муайян рискларни жойлаштиради ва контекстни ўрнатишда аниқланган рискларни баҳолаш мезонлари бўйича уларни таснифлайди. РИСКНИ аниқлаш кўпинча икки (ёки ундан кўп) итерациядан фойдаланиб ўтказилади.

Рискларни аниқлашнинг мақсад ва вазифалари асосида рискларни аниқлашга ўз ёндашувини танлаш ташкилотнинг ўзига боғлиқ.

Рискларни идентификация қилишдэн мақсад, потенциал зарар етказадиган эҳтимолий инцидентларни прогнозлаш ва бу зарар қай тарзда олиниши мумкинлиги тўғрисида тасаввурга эга бўлиш ҳисобланади. Қуйида тавсифланган қадамлар рискларни таҳдил қилиш бўйича табдирлар учун кириттт маълумотларини аниқлайди.

Рискларни идентификация қилишдан мақсад, потенциал зарар етказадиган эҳтимолий инцидентларни прогнозлаш ва бу зарар қай тарзда олиниши мумкинлиги тўғрисида тасаввурга эга бўлиш ҳисобланади. Қуйида

тавсифланган қадамлар рискларни таҳлил қилиш бўйича табдирлар учун кириш маълумотларини аниқлайди.

Активларни аниқлашда ахборот тизими фақат аппарат ва дастурий воситалардан иборат эмаслигини назарда тўтиш керак. Активларни аниқлаш рискларни баҳолаш учун етарли ахборот таъминланадиган тегишли деталлаштириш даражасида амалга оширилиши зарур. Активларни аниқлашда фойдаланиладиган деталлаштириш даражаси рискларни баҳолаш вақтида тўпланган ахборотнинг умумий ҳажмига таъсир этади. Бу даража рискларни баҳолашнинг кейинги итерацияларида янада деталлаштирилиши мумкин.

Киберхавфсизлик соҳасидаги фактлар:

Кучли пароль кўп ҳужумларни бартараф этиши мумкин.

Янги восита (дастурий-аппарат) хавфсиз ҳисобланмайди.

Энг яхши дастурий воситалар заифликларни ўз ичига олади.

Булутли технология тўлиқ хавфсиз эмас.

Хакералар-булар ҳама вақт ҳам жиноятчи эмас.

Компьютер ва компьютер тармоқларида компьютер хавфсизлиги инцидентларини бошкарнш ўз ичига мониторинг ва хавфсизлик ҳодиса-воқеаларини, ҳамда бу ҳодиса-воқеаларга тўғри жавобларни қайтаришни қамраб олади. Инцидентни бошқариш дастур ҳисобланиб маълум бир жараённи аниқлаб беради ва амалга оширади.

Ҳодиса - шахс ёки итттчи жараённи, жараённи, ўраб олган мухит ва тизимни нормал ҳолатини ўзгартиришни назорат этишдир.

Ҳодисанинг учта асосий тури мавжуд:

Нормал. Нормал ҳодиса критик компоненталарга таъсир қилмайди ёки кўрсатма (резолюция)ни бошланишидан олдин ўзгартиришни назорат этишни талаб қилади.

Ҳодисаларни кенгайиши ва кўпайиши (Эскалация). Ҳодисаларни кўпайиши тизимга жиддий таъсир кўрсатади ёки амалга оширилган кўрсатма (резолюция) ўзгартиришни назорат этиш жараёнини кузатишини таъминлаб бериши шарт.

Авариявий ҳодиса. Авариявий ҳодиса шахс хавфсизлиги ва соғлигига таъсир кўрсатади.

Инцидент - бу стандарт операциялар қаторига қўшилмайдиган ҳамда хизмат ҳолатини узиб қўйиш ёки хизмат сифати ёмонлашиши ҳолатларига олиб келадиган ҳар қандай ҳодисага айтилади.

Инцидентга жавоб қайтариш гуруҳи. Хавфсизлик инциденти координатори инцидентга жавоб қайтариш жараёнини бошқаради ва командани тўплаш учун жавобгар шахсдир. Координатор командани ташкил этиб, ташкил этилган команда ўз ичига инцидентни баҳоловчи ва қарор қабул қилувчи шахсларни қамраб олади.

Инцидентни тергов қилиш - бу инцидент ҳолатини тергов қилиш ҳаракатидир. Ҳар бир инцидент тергов этишни талаб қилиши ёки унга кафиллик бериши керак бўлади. Шу билан бирга тергов қилинадиган

ресурслар, яъни тиббий воситалар, номуносиб тармоқлар ва карантин қилинган тармоқлар фавқулодда инцидентларга тез ва самарали рухсат бериш учун фойдали ҳисобланади.

Инцидентга жавоб қайтариш - бу хавфсизликни бузилиш кетма-кетлиги ёки ҳужумни бошқариш ва ечиш учун ишлаб чиқилган усулдир. Бунинг мақсади вазиятни тўғрилаш, яъни тизимни бузилишини чеклаш ва бузилган тизимни тиклаш вақти ва маблағини камайтиришдир.

Инцидент бошқарувчисини вазифалари ва мажбуриятлари:

муносиб ваколатлардан фойдаланиш учун ҳар қандай авария / носозликларни билиш;

етарли ахборот йиғиш ва тизимни таҳлил этиш учун қайта тиклайдиган командани шакллантириш;

инцидентни умумий ҳолатини сақлаш;

Кўп ташкилот ва корхоналарда ахборот хавфсизлиги инцидентларни бошқариш жараёин қуйидагича қурилади:

компьютер инциденти ҳақида ахборот олиш;

қоидабузарлик аниқланган ҳолатларда қўшимча ахборот олиш;

ҳолатни таҳлил этиш;

сабабларни аниқлаш;

профилактик тадбирлар ўтказиш.

Инцидентларини бошқариш жараёни самарадорлиги қўйидагиларга боғликдир:

ахборот хавфсизлиги инцидентини бошқариш жараёнида жалб этилган шахсларнинг тизимни бошқаришни яхши билиши;

инцидент билан боғлиқ ахборотни таҳлил этиш ва олиш имкониятларнинг борлиги;

олинган натижаларнинг ҳақиқийлиги.

Инцидентини бошқариш тизимини қуриш концепцияси ва структурасини қараб чиқамиз.

Ахборот хавфсизлиги инцидентини бошқариш тизими архитектураси қуйидаги асосий компоненталарни ўз ичига олади:

Интеграллашган платформа.

Аудит ва мониторингни аппарат-дастурий воситалари.

Ахборотни ҳимоялашнинг аппарат-дастурий воситалари.

Ахборот хавфсизлиги инцидентлари ҳақида ахборот омбори.

Ҳисоботларни генерациялаш воситалари ва аналитик асбоблар.

Воситаларни бошқариш ва интерфейсни тўғрилаш.

Интеграллашган платформа тизимнинг ядроси ҳисобланади. Бу тизим тузилишидаги ҳамма компоненталарни битта умумий функцияга боғлаб беради.

Интеграллашган платформа қўйидагилардан таркиб топган:

Маълумотларни йиғишни таъминловчи мониторинг ва аудит воситалари учун интерфейс.

Ахборот хавфсизлиги инцидентлари оқибатини локализациялаш мақсадида конфигурацияни тезкор ўзгартиришдаги ахборот ҳимояси воситалари интерфейси

Ҳисоботларни генерациялаш воситалари ва аналитик функциялардан фойдаланишдаги хизматлар.

Аудит ва мониторингни аппарат-дастурий воситалари - ташкилот ахборот тизимини қайта ишлаш, йиғиш ва протоколлаштиришни амалга оширувчи воситалардир. Бу воситаларга қуйидагилар киради: ўрнатилган воситалар

(иловалар, операцион тизим воситалари, тармоқ қурилмалари, ҳимоя воситалари ва автоматлаштирилган тизимлар) ва махсус воситалар (аудит, хавфсизлик сканерлари, дастурий агентлар, сенсорлар, ахборот йиғувчи қурилмалар).

Кодлаштириш деб, ахборотни бир тизимдан бошқа тизимга маълум бир белгилар ёрдамида белгиланган тартиб бўйича ўтказиш жараёнига айтилади.

Криптография деб махфий хабар мазмунини шифрлаш, яъни маълумотларни махсус алгоритм бўйича ўзгартириб, шифрланган матнни яратиш иули билан ахборотга рухсат этилмаган киришга тўсиқ қўйиш усулига айтилади.

Калит- матнни шифрлаш ва шифрини очиш учун керакли ахборот.

Криптоанализ - калитни билмасдан шифрланган матнни очиш имкониятларини ўрганади.

Криптография ҳимоясида шифрларга нисбатан қуйидаги талаблар қўйилади:

етарли даражада криптобардошлилик;

шифрлаш ва қайтариш жараёнининг оддийлиги;

ахборотни шифрлаш оқибатида улар ҳажмининг ортиб кетмаслиги;

- шифрлашдаги КИЧИК хатоларга таьсирчан бўлмаслиги.

Шифрлаш ва дешифирлаш масалаларига тегишли бўлган, маълум бир алфавитда тузилган маълумотлар матнларни ташкил этади. Алфавит - ахборотларни ифодалаш учун фойдаланиладиган чекли сондаги белгилар тўплами. Мисоллар сифатида:

- ўттиз олтита белгидан (ҳарфдан) иборат ўзбек тили алфавити;
- ўттиз иккита белгидан (ҳарфдан) иборат рус тили алфавити;
- йигирма саккизта белгидан (ҳарфдан) иборат лотин алфавити;
- икки юзи эллик олтита белгидан иборат А8СП компьютер белгиларининг алфавити;
- бинар алфавит, яъни 0 ва 1 белгилардан иборат бўлган алфавит;
- саккизлик ва ўн олтилик саноқ системалари белгиларидан иборат бўлган алфавитларни келтириш мумкин.

Симметрик шифрларда маълумотни шифрлаш ва дешифрлаш учун бир ХИЛ калитдан фойдаланилади.

Бундан ташқари очиқ калитли (ассиметрик) криптотизимлар мавжуд бўлиб, унда шифрлаш ва дешифрлаш учун иккита калитдан фойдаланилади.

Стенография - бу махфий хабарни сохта хабар ичига беркитиш орқали алоқани яшириш ҳисобланади. Бошқа сўз билан айтганда стеганографиянинг асосий ғояси - бу махфий маълумотларнинг мавжудлиги ҳақидаги шубҳани олдини олиш ҳисобланади.

Хулоса ўрнида шуни айтиш мумкинки, симметрик калитли ва очиқ калитли криптотизимлар маълумотларни махфийлигини таъминлашда фойдаланилса, хэш функциялар эса маълумотни бутунлигини текширишда фойдаланилади.

Муҳим маълумотларни ҳимоя қилиш масаласида кўпинча маиший ёндашиш ишлатилади: «касалликни даволагандан кўра унинг олдини олган яхшироқ». Афсуски, айнан у энг бузувчи оқибатларни келтириб чиқаради. Компьютерга вирусларни кириб олиш йўлида баррикадаларни яратиб олиб, уларнинг мустаҳкамлигига ишониб ва бузувчи ҳужумдан кейинги ҳаракатларга тайёр бўлмасдан қолмаслик керак. Шу билан бирга, вирусли ҳужум, бу муҳим маълумотларни йўқотишни ягона бўлмаган ҳаттоки кенг тарқалмаган сабабидир. Шундай дастурли узилишлар мавжудки, улар операцион тизимни ишдан чиқариши мумкин ҳамда шундай аппаратли узилишлар борки, улар қаттиқ дискни ишлашга лаёқатсиз қилиб қўйиш қобилиятига эгадирлар. Ўғирлаш, ёнғин ёки бошқа фавқулодда ҳолатлар натижасида муҳим маълумотлар билан биргаликда компьютерни йўқотиш эҳтимоли ҳар доим ҳам мавжуддир. Шунинг учун хавфсизлик тизимини яратишни биринчи навбатда «охиридан» бошлаш керак - исталган таъсирни, у вирус ҳужуми, хонада ўғирлик ёки қаттиқ дискни физик ишдан чиқишидан қатъий назар, бузувчи оқибатларини бартараф этишдан бошлаш керак.

Маълумотлар билан ишончли ва хавфсиз ишлашга фақат шундагина эришиладики, агар исталган кутилмаган ҳодиса, шу жумладан компьютерни тўлиқ физик ишдан чиқариш ҳам, салбий оқибатларга олиб келмаслиги керак.

Адабиётлар ва интернет сайтлар:

1. Dileep Kumar G, Manoj Kumar Singh and M.K. Jayanthi. Network Security

Attacks and Countermeasures. Indexed In: SCOPUS |Copyright: © 2016 |Pages: 357

2. Phillip Ferraro. Cyber Security: Everything an Executive Needs to Know. Hardcover – July 6, 2016.

3. Ахборот хавфсизлиги бўйича ўқув-услубий мажмуа. https://studfile.net/preview/7883185/

4. https://studfile.net/preview/7883185/page:23/