КОРХОНАЛАРНИНГ АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ

Ишназаров.А
Тошкент давлат иқтисодиёт университети Иқтисодиётда математик методлар кафедраси доценти
Тўқумбетов.О
Тошкент давлат иқтисодиёт университети Рақамли иқтисодиёт факультети талабаси

Аннотация: *Ушбу мақолада корхоналарда ахборот хавфсизлигини таъминлаш масалалари ёритилган. Корхона учун ахборот таҳдидларининг турлари, уларни аниқлаш усуллари ҳамда корхонанинг ахборот хавфсизлигини таъминлаш учун қўлланиладиган ташкилий чора-тадбирлар ёритиб берилган.*

Калит сўзлар: *ахборот хавфсизлиги, ташқи ҳужумлар, DPL тизимлари, Хакерлар, аутентификация ва идентификация тизими.*

Маълумки, компьютерларнинг инсон фаолиятининг турли соҳаларига жорий этилиши электрон шаклда сақланадиган ахборот ҳажмининг катта ҳажмларга кўпайишига олиб келди. Бу жараёнлар, шубҳасиз, ўзини оқлади, чунки ахборотни электрон шаклда сақлаш осонроқ, катта ҳажмдаги маълумотларни тезда нусхалаш, қайта ёзиш ва узоқ масофаларга узатиш мумкин. Бироқ, компьютерни глобал тармоқларга улашнинг салбий томонлари ҳам бор - ахир, тегишли ҳимоя даражаси бўлмаса, маълумотлар тармоқ ёки Интернет орқали ҳужумлардан бузилиши мумкин.

Тижорат маълумотларининг йўқолиши ёки унинг тажовузкорлар ёки рақобатчилар томонидан ошкор этилиши корхонанинг бозордаги йўқотишларига олиб келиши мумкин. Демак, ахборотни ўғирлаш корхона обрўсини пасайтириши мумкин, маълумот ўрнини босишга келсак, бу ҳатто мижозлар ишончини ҳам йўқ қилишга олиб келиши мумкин [1].

Корхоналар учун ахборот хавфсизлиги тизимини яратиш вазифаси мураккаб. Раҳбарият идрок этилган хавфлар даражасини баҳолаши ва таҳдид моделини ишлаб чиқиши керак. Бу бизнеснинг ҳар бир тури учун ҳар хил бўлади. Умумий нарса шундаки, ахборот технологиялари корхонага зарар етказиш учун ишлатилади. Ахборот хавфсизлигини таъминлаш учун аудит ўтказиш керак, унинг натижалари бўйича зарур ташкилий ва дастурий-техник чора-тадбирлар комплекси ишлаб чиқилади.

Ахборот хавфсизлигига таҳдидларга келадиган бўлсак, хакерлик ҳужумлари халқаро даражада жамиятни рақамлаштириш билан боғлиқ ягона глобал таҳдиднинг бир қисми сифатида кўриб чиқилади. Ҳатто кичик корхоналар ҳам ташқи ҳужумлардан озод этилмайди, айниқса улар йирик

корхоналарнинг етказиб берувчилари ёки пудратчилари бўлса ва ўз фаолиятида тажовузкорлар учун қизиқарли бўлиши мумкин бўлган маълумотлар билан ишласа [3,4,6].

Ахборот хавфсизлигига жорий ташқи таҳдидлар орасида:

• ахборот тизимини бузиш ёки ёмон ҳимояланган алоқа каналларига уланиш орқали махфий маълумотларни ўғирлаш. DPL тизимлари маълумотларнинг сизиб чиқишидан энг яхши тарзда ҳимоя қилади, аммо барча кичик ва ўрта бизнес ўз ресурсларидан тўлиқ фойдаланиш имкониятига эга эмас;

• шахсий маълумотларни ўз аутентификация воситаларидан фойдаланган ҳолда ўғирлаш ва уларни қора ахборот бозоридаги воситачиларга топшириш. Ушбу турдаги таҳдид энг кўп мижоз маълумотларини қайта ишлайдиган банклар ва хизмат кўрсатиш ташкилотлари учун одатий ҳисобланади;

• рақобатчиларнинг илтимосига биноан инсайдерлар томонидан тижорат сирларини ўғирлаш, кўпинча улар ташкилот мижозларининг маълумотлар базаларини ўғирлаш;

• алоқа каналларини бузишга қаратилган DDoS ҳужумлари. Улар компаниянинг веб-сайтига кириш имкони бўлмайди, бу Интернетда товарлар сотадиган ёки хизматлар кўрсатадиган ташкилот учун жуда муҳимдир;

• вирусли инфекциялар. Сўнгги пайтларда тизимдаги маълумотларга кириш имкони бўлмаган ва уни тўлов учун қулфдан чиқарадиган энг хавфли шифрлаш вируслари. Баъзан, кузатиш имкониятини бартараф этиш учун хакерлар криптовалюталарда мукофот тўлашни талаб қиладилар;

• сайтни бузиш. Ушбу турдаги хакерлик ҳужуми билан ресурснинг биринчи саҳифаси баъзан ҳақоратли матнларни ўз ичига олган бошқа контент билан алмаштирилади;

• фишинг. Компьютер жиноятларини содир этишнинг бу усули тажовузкорнинг мухбир манзилига ўхшаш манзилдан хат юборишига, уларни ўз саҳифасига киришга ва парол ва бошқа махфий маълумотларни киритишга ундашига асосланади. ўғирланган;

• кирувчи алоқа каналларини спам блоклаш ва муҳим ёзишмаларни кузатишни олдини олиш;

• компания ходимларини тажрибали фирибгар фойдасига ресурсларни ўтказишга ундайдиган ижтимоий муҳандислик воситалари;

• аппаратдаги носозликлар, ускунанинг ишламай қолиши, бахтсиз ҳодисалар, табиий офатлар натижасида маълумотлар йўқолиши.

Таҳдидларнинг умумий рўйхати ўзгаришсиз қолмоқда ва уларни амалга оширишнинг техник воситалари доимий равишда такомиллаштирилмоқда. Ахборот тизимларининг мунтазам компонентларидаги заифликлар (ОТ, алоқа протоколлари) ҳар доим ҳам тезда бартараф этилмайди. Хакерлар

барча янгиланишларга тезда жавоб бериш учун вақтни беҳуда сарфламайдилар, мониторинг воситаларидан фойдаланган ҳолда корпоратив ахборот тизимларининг хавфсизлик даражасини доимий равишда синаб кўришади. Улар ахборот ҳужумларида фаол иштирок этадилар, чунки уларни бошқарадиган дастурий таъминот ишлаб чиқарувчилари пулни тежаш учун уларга назоратни ушлаб қолишдан ҳимоя қилиш механизмини ўрнатмаганлар.

Корхоналарнинг ахборот хавфсизлигини таъминлаш вазифаси мустақил равишда ёки ташқи экспертларни жалб қилган ҳолда ҳал қилинади [2,5]. Аудит ўтказиш ва корхонанинг ахборот хавфсизлигининг юқори сифатини самарали таъминлайдиган умумий ва махсус характердаги ташкилий-техник тадбирлар тизимини жорий этиш зарур. Аудит билан тизим яратишни бошлаш керак. Ҳимоя тизими унинг натижаларига асосланади.

Аудитнинг кўлами корхонанинг ҳажмига ва қайта ишланаётган маълумотларнинг қийматига боғлиқ. Кичик ва ўрта бизнес учун аудит ўз-ўзидан амалга оширилиши мумкин, юқори аҳамиятга эга бўлган махфий маълумотлар қайта ишланадиган бир нечта назорат даврларини ўз ичига олган тақсимланган комплекс тизим учун маълумотларни аутсорсингга ихтисослашган профессионал ташкилотларни жалб қилиш керак. аудит учун хизматлар.

Аудитнинг асосий даражасида қуйидагиларни аниқлаш керак:

• компьютерлар маълум бир бўлим ходимларидан бошқа ҳар ким учун мавжудми ёки йўқми, кириш тизими электрон рухсатномалар ёрдамида амалга оширилганми ва ходимнинг хонада бўлган вақтини белгилаш;

• олинадиган ташувчини иш станцияларига улаш мумкинми, олинадиган қурилмаларга маълумотларни нусхалашнинг жисмоний қобилияти;

• ахборот тизимининг иш станцияларида қандай дастурий таъминот ўрнатилган, у лицензияланганми, янгиланишлар мунтазам равишда амалга ошириладими, ўрнатилган дастурий таъминотнинг ташқаридан маълумотларга киришни осонлаштирадиган маълум камчиликлари борми;

• операцион тизим қандай конфигурация қилинганлиги, корпоратив ахборот хавфсизлигининг мунтазам ресурслари, антивируслар, хавфсизлик девори, фойдаланувчи ҳаракатлари журнали, киришни бошқариш воситаларидан фойдаланилади;

• фойдаланиш ҳуқуқларини табақалаш тизими қандай амалга оширилганлиги, имкон қадар камроқ ҳуқуқлар бериш тамойили қўлланиладими, фойдаланиш ҳуқуқларига ким ва қандай ўзгартиришлар киритилади;

• аутентификация ва идентификация тизими қандай амалга оширилганлиги, икки факторли модел қўлланиладими, логин ва паролларни бошқа ходимларга ўтказиш учун жавобгарлик борми;

• парол тизими қандай амалга оширилади, улар қанчалик тез-тез ўзгартирилади, тизим паролни қайта-қайта нотўғри киритишга қандай муносабатда бўлади.

Баъзида таҳдидлар тасодифий ва олдиндан айтиб бўлмайдиган бузғунчиликлардан кўра муҳимроқ бўлган ҳолатлар мавжуд, масалан, корхона:

• юқори рақобатбардош бозорда ишлайди;

• илмий ёки ахборот технологияларини ишлаб чиқишда иштирок этади;

• катта ҳажмдаги шахсий маълумотларни қайта ишлайди.

Бундай ҳолларда кириш ва дастурий таъминотнинг ўзига хослигини текшириш муаммони ҳал қилмайди. Ахборот тизимини янада чуқурроқ ўрганиш керак ва қуйидагиларни аниқлаш керак:

• пуллик ва бепул дастурлар - сканерлари ёрдамида ташқи киришлар учун тизим заифликларининг мавжудлигини;

• ахборот тизимининг алоҳида кластерларида юқори даражадаги махфийлик билан маълумотларни қайта ишлашнинг йўқлиги ёки мавжудлиги, зоналар чегараларида ўрнатилган хавфсизлик деворини;

• масофавий ходимлардан маълумотларни узатишда хавфсиз алоқа протоколларидан фойдаланишини;

• фойдаланувчиларнинг махфий маълумотларни ўз ичига олган объектлар билан қилган ҳаракатлари қандай қайд этилганлигини;

• маълумотларга табақалаштирилган кириш амалга ошириладими, қандай усул қўлланилади, кўп даражали кириш тизими мавжудлигини.

Аудит саволларига жавоб тегишли таҳдидларни ҳисобга олган ҳолда корхона ахборот хавфсизлиги тизимини ривожлантириш учун асос бўлади.

Корхоналарда ахборот хавфсизлигини таъминлаш учун хавфсизлик тизимини жорий этиш лозим. Корхонада хавфсизлик тизимини жорий этиш босқичлари қуйидагилар [2,4].

Иш қуйидаги алгоритмга мувофиқ амалга оширилиши керак:

• ахборот тармоғи архитектурасида барча инфратузилма ва дастурий таъминот объектларининг тавсифи, уларнинг асосий характеристикаларини аниқлаш;

• вақт, инсон ва бюджет чекловларини ҳисобга олган ҳолда ахборот тизимининг оптимал конфигурациясига қўйиладиган талабларни ишлаб чиқиш;

• ташкилий-маъмурий ҳужжатлар тўпламини ишлаб чиқиш, у билан ходимларни таништириш, уларни ахборот хавфсизлиги асосларига ўргатиш;

• ахборот хавфсизлиги инцидентларининг юзага келишининг олдини олиш ва уларга жавоб чораларини янада самаралироқ қилишга қаратилган техник ва дастурий чора-тадбирларни амалга ошириш.

Бутун жараёнга корхонанинг ахборот хавфсизлиги стратегиясини амалга ошириш лойиҳасини муваффақиятли амалга оширишдан манфаатдор бўлган менежер раҳбарлик қилиши керак.

Корхонанинг ахборот хавфсизлигини таъминлаш учун қўлланиладиган ташкилий чора-тадбирлар уч гуруҳга бўлинади:

• мажбурий характер;

• шахсий маълумотларни ҳимоя қилиш;

• алоҳида ахборот объектлари ёки жараёнларини ҳимоя қилиш.

Ҳар бир тоифа доирасида улар икки гуруҳга бўлинади - ҳужжатлар ва ҳаракатлар ва ҳар бир ҳимоя секторида иккала чора гуруҳи ҳам зарур.

Корхонанинг ахборот хавфсизлиги маълумотлар ҳимоясини таъминлаш бўйича ягона сиёсат ёки методологияни қабул қилишдан бошланади. Сиёсат қуйидаги бўлимларни ўз ичига олиши керак:

• ахборот хавфсизлигининг умумий тамойиллари, таҳдидлар ва хавфсизлик мақсадлари;

• маълумотларнинг компания учун аҳамиятлилик даражасига кўра таснифи;

• маълумотларга кириш шартлари, фойдаланишни бошқариш тамойиллари;

• компьютерлар ва олинадиган ташувчилар билан ишлаш қоидалари;

• ҳужжатлар талабларини бузганлик учун жавобгарлик.

Ҳужжат юқори бошқарув даражасида қабул қилинади ва корхонада ахборот хавфсизлигини таъминлаш бўйича аниқроқ вазифаларни белгилайдиган сиёсат ва усуллар билан бирга келади.

Ахборотни ҳимоя қилишнинг дастурий ва аппарат воситаларини жорий этиш муқаррар, кўпгина ташкилотлар уларни билмаган ҳолда ишлатадилар. Муайян ташкилот учун энг самарали ҳимоя турларини танлаш учун қуйидаги саволларга жавоб бериш керак [2,3,6]:

• ҳимоя қилинадиган ахборот турлари, тармоқнинг қайси секторларида ва қайси маълумотлар базаларида сақланади. Корхона фаолиятида энг муҳим маълумотлар корпоратив банк карталари ва ҳисоб рақамлари, шахсий маълумотлар, бизнес сирлари, мижозларнинг маълумотлар базалари тўғрисидаги маълумотларни ўз ичига олади, улар кўпинча қасддан ўғирлашга қаратилган;

• тармоқ инфратузилмасини яратишда қайси қурилмалар иштирок этади ва унга масофавий уланиш орқали қайси қурилмалар уланади, ким ва қандай асосда уланишга рухсат беради;

• қандай дастурий таъминотни алмаштириш ёки янгилаш керак, қандай қўшимча хавфсизлик модулларини ўрнатиш керак;

• администратор аккаунтлари қандай ҳимояланганлиги, бошқа шахс паролларни тахмин қилиш орқали улардан фойдаланиши мумкинми ёки бошқача тарзда;

• файллар ёки трафикни шифрлаш зарурати борми, бунинг учун қандай воситалар қўлланилади;

• вирусга қарши дастурлар, электрон почтани фильтрлаш дастурлари, хавфсизлик девори замонавий хавфсизлик талабларига жавоб берадими;

• ходимларнинг интернетга кириши қандай тартибга солинади, махсус рухсат олиш керакми, қайси сайтлар блокланади ва бошқалар.

Кейинчалик, самарали даражада корпоратив ахборот хавфсизлиги тизимини яратиш учун мўлжалланган дастурий таъминотни танлаш босқичи бошланади:

• антивирус ҳимояси;

• хавфсизлик деворлари (файрволлар). Бу ерда Ўзбекистонда тасдиқланган дастурий маҳсулотларга эътибор қаратиш тавсия этилади;

• ходимларнинг почта қутиларини спам ва вируслардан ҳимоя қилувчи электрон почтани филтрлаш воситалари;

• компьютерларида ўрнатилган Enhanced Mitigation Experience Toolkit (EMET) код билан боғлиқ заифликлардан ҳимоя қилишда фойдали бўлади;

• криптографик ҳимоя воситалари. Маълумотларнинг махфийлиги даражасига қараб, оммавий фойдаланиш мумкин бўлган маҳсулотлар қўлланилади;

• инфратузилманинг иш қобилиятини мониторинг қилиш воситалари. Бепул ёки лицензияланган маҳсулотлар танланиши мумкин, асосийси заифликларнинг доимий мониторингини ўрнатишдир;

• ахборотнинг сизиб чиқишига қарши кураш воситалари. Ахборот ҳимояси периметридан махфий маълумотларни олишга ҳар қандай уринишларни блокировка қилиш учун тузилган DLP тизимини ўрнатиш мумкин.

Корхонанинг ахборот хавфсизлиги учун асосий хавфлардан бири дастурий таъминотни ўз вақтида янгилашдан бош тортишдир. Бир нечта сабаблар бўлиши мумкин [2]:

• тизим маъмурларининг эътиборсизлиги;

• чекланган бюджет;

• шахсий маълумотларни ҳимоя қилиш учун фойдаланиладиган дастурий таъминотни сертификатлашнинг узоқ муддати.

Аммо дастурий таъминотни ўз вақтида янгилаш хакерлар учун бўшлиқлар яратади, бу эса маълумотларнинг сизиб чиқишига олиб келиши мумкин. Агар бундай хавфлар мавжуд бўлса, Windows учун қайси янгиланишлар ўрнатилмаганлигини ва хавфсизликни таъминлаш учун

қандай конфигурация ўзгаришларини киритиш кераклигини аниқлаш учун Microsoft Security Analyzer дастуридан фойдаланиш мумкин.

Қурилманинг уланишини текширишда қуйидаги усуллардан фойдаланиш керак:

• маршрутизатор (симсиз уланиш контроллери) ёрдамида тармоққа қайси қурилмалар уланганлигини текшириш;

• каттароқ тармоқлар учун қурилмаларни қидиришда тармоқ сканеридан фойдаланиш мумкин;

• қурилмаларни тармоққа улаш билан боғлиқ барча ҳодисаларни қайд қилишни фаоллаштириш.

Оддий тавсияларни амалга ошириш корхонанинг ахборот хавфсизлигини кафолатланган ҳимоя тизимини ва ҳодисаларнинг йўқлигини таъминлайдиган даражада яратишга имкон беради.

Юқорида келтириб ўтилган хавфларни олдини олиш учун албатта корхонада ушбу вазифаларни бажарувчи юқори малакали ИТ-мутахассислари бўлиши ҳамда улар ушбу соҳадаги янгиликлардан хабардор бўлиб туришлари муҳим ҳисобланади.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ:

1. Карзаева Н.Н. Основы экономической безопасности: учебник. –М.: Инфра-М, 2017. – 275 с.

2. Информационная безопасность предприятия: учеб. пособие. –М.: ФОРУМ: Инфра-М, 2017. – 239 с.

3. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. –М.: Риор, 2017. - 476 с.

4. Ganiev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi. –T.: “Fan va texnologiya”, 2016. – 372 b.

5. Ganiev S.K., Ganiev A.A., Xudoyqulov Z.T. Kiberxavfsizlik asoslari. O‘quv qo‘llanma. –T.: “Aloqachi”, 2020. – 221 b.

6. Karimov I.M., Turgunov N.A. Axborot xavfsizligi asoslari. –T.: O‘zbekiston Respulikasi IIV Akademiyasi, 2016. – 91 b.