«БЕКІТЕМІН»
Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті Академиялық инновация және жоғары білімнен кейінгі білім беру ісі жөніндегі вице-президент, Сапа бойынша басшылық Өкілі
_____ Ш.Есимова
«30» 01 2020 ж.

САПА МЕНЕДЖМЕНТІНІҢ ЖҮЙЕСІ

ЖҰМЫС НҰСҚАУЫ
ЖН-СМЖ-004-2020

ШТАТТАН ТЫС (ДАҒДАРЫСТЫҚ) ЖАҒДАЙЛАРДА ПАЙДАЛАНУШЫЛАРДЫҢ ІС-ҚИМЫЛ ТӘРТІБІ ТУРАЛЫ НҰСҚАУЛЫҚ

АЛҒЫ СӨЗ

1. IT Департаментімен ӘЗІРЛЕНДІ ЖӘНЕ ЕНГІЗІЛДІ

2. Әзірлегендер – IT Департаментінің директоры Т.Карипов
– Директор орынбасары А.Кожихов

3. Келісілді – Оқу-әдістемелік ісі жөніндегі вице президент Ө.Умбетов
– Құқықтық қамтамасыз ету бөлімінің басшысы Г.Мусаханов
– Стратегиялық жоспарлау, рейтинг және сапа орталығының басшысы Ж.Дарибаев

4. ЕНГІЗІЛДІ – 2020 ж.
5. Тексерілу мерзімі – 2022 ж.

ҚА Ясауи атындағы ХҚТУ Сапа менеджменті басқармасы ТЕКСЕРІЛДІ: «07» 02 2022ж.
КЕЛЕСІ ТЕКСЕРУ: «07» 02 2024ж.
ҚА Ясауи атындағы Халықаралық Қазақ-Түрік университетінің Сапа менеджментінің жүйесі БАҚЫЛАУ ДАНАСЫ № 77 «30» 01 2020ж.

Қызмет бабында пайдаланатын басылым

Түркістан

1. ЖАЛПЫ ЕРЕЖЕЛЕР

Осы Нұсқаулық Университеттің ақпараттық жүйесінде (бұдан әрі-АЖ) штаттан тыс жағдайлар/инциденттер туындаған кезде іс-қимыл тәртібін ұйымдастыруға арналған.

Штаттан тыс жағдайды/инциденттерді жою бойынша іс-шараларды жүргізу кезіндегі іс-қимылдарды бақылау және үйлестіру ат департаментіне жүктеледі.

Бұл Нұсқаулықта келесі мәселелер қарастырылады:

1. Қауіпсіздікке төнетін қауіп көздері және олардың түрлері;
2. Дағдарыстық жағдайлар және Санаттар;
3. АЖ үздіксіз жұмысын және жұмыс қабілеттілігін қалпына келтіруді қамтамасыз ету шаралары;
4. Дағдарыстық жағдай туындаған кездегі жалпы талаптар;
5. Ақпараттық қауіпсіздік инциденттерін басқару;
6. Инцидент туралы хабарлау фактісі бойынша іс-қимылдардың жалпы сценарийі;
7. Ақпараттық қауіпсіздік инциденттерін басқару рәсімдері.

2. ҚАУІПСІЗДІККЕ ТӨНЕТІН ҚАУІП КӨЗДЕРІ

АЖ мен ақпараттың қауіпсіздігіне төнетін қатерлердің негізгі көздері мыналар болып табылады:

1. табиғи апаттар мен авариялар (су тасқыны, дауыл, жер сілкінісі, өрт және т. б.);
2. АЖ жабдықтарының (техникалық құралдарының) істен шығуы және істен шығуы;
3. АЖ компоненттерін жобалау және әзірлеу қателері (аппараттық ақпаратты өңдеу құралдары, технологиялары, бағдарламалар, деректер құрылымы және т. б.);
4. пайдалану қателері (пайдаланушылар, операторлар және басқа қызметкерлер);
5. бұзушылар мен қаскүнемдердің қасақана іс-әрекеттері;

Бұл ретте қауіптер табиғи және жасанды 2 түрге бөлінеді:

Табиғи қауіптер - бұл АЖ-ға және оның элементтеріне, адамға тәуелсіз объективті физикалық процестерге немесе табиғи құбылыстарға әсер етуден туындаған қауіптер.

Жасанды қауіптер - бұл адамның іс-әрекетінен туындаған АЖ-ға төнетін қауіптер. Олардың ішінде іс-әрекеттің мотивациясына сүйене отырып, мыналарды бөлуге болады:

- АЖ-ны және оның элементтерін жобалаудағы қателіктерден, бағдарламалық қамтамасыз етудегі қателіктерден, персонал іс-әрекеттеріндегі қателіктерден және т. б. туындаған абайсызда (абайсызда, кездейсоқ) қауіптер.

Негізгі абайсызда жасанды қауіптер:

1) жүйенің ішінара немесе толық істен шығуына немесе жүйенің аппараттық, бағдарламалық, ақпараттық ресурстарының бұзылуына әкеп соғатын абайсыз іс-әрекеттер (жабдықты байқаусызда бүлдіру, маңызды ақпараты бар файлдарды немесе бағдарламаларды, оның ішінде жүйелік және т. б. жою, бұрмалау);

2) Жабдықты заңсыз ажырату немесе құрылғылар мен бағдарламалар жұмысының режимдерін өзгерту;

3) ақпарат тасымалдағыштарды байқаусызда бүлдіру;

4) біліксіз пайдалану кезінде жүйенің жұмыс қабілеттілігін жоғалтуды тудыратын (ілініп қалу немесе ілмектеу) немесе жүйеде қайтымсыз өзгерістерді жүзеге асыратын (ақпарат тасымалдағыштарды форматтау немесе қайта құрылымдау, деректерді жою және т. б.) технологиялық бағдарламаларды іске қосу;

5) кейіннен ресурстарды негізсіз жұмсай отырып, ескерілмеген бағдарламаларға (ойын, оқыту, технологиялық және т. б., өзінің қызметтік міндеттерін бұзушының орындауы үшін қажетті болып табылмайтын) санкцияланбаған қол жеткізу және пайдалану (процессорды жүктеу, жедел жадыны және сыртқы жеткізгіштердегі жадты басып алу);

6) компьютерді вирустармен жұқтыру;

7) құпия ақпаратты жария етуге әкеп соғатын немесе оны жалпыға қолжетімді ететін абайсыз әрекеттер;

8) қол жеткізуді шектеу атрибуттарын (парольдерді, шифрлау кілттерін, сәйкестендіру карточкаларын, рұқсаттамаларды және т. б.) жария ету, беру немесе жоғалту.);

9) жүйенің архитектурасын, деректерді өңдеу технологиясын жобалау, жүйенің жұмыс қабілеттілігі мен Ақпарат қауіпсіздігі үшін қауіп төндіретін мүмкіндіктермен қолданбалы бағдарламаларды әзірлеу;

10) жүйеде жұмыс істеу кезінде ұйымдастырушылық шектеулерді (белгіленген ережелерді) елемеу;

11) қорғаныс құралдарын айналып өтіп жүйеге кіру (ауысымды магнитті тасығыштардан бөгде операциялық жүйені жүктеу және т. б.);

12) қауіпсіздік қызметі персоналының қорғау құралдарын біліксіз пайдалануы, күйге келтіруі немесе заңсыз ажыратуы;

13) абоненттің (құрылғының) қате мекенжайы бойынша деректерді жіберу;

14) қате деректерді енгізу;

15) байланыс арналарына байқаусызда зақым келтіру.

16) адамдардың (қаскүнемдердің) пайдакүнемдік, идеялық немесе өзге де ұмтылыстарына байланысты қасақана (қасақана) қатерлер.

Негізгі қасақана жасанды қауіптер:

Жұмысты қасақана іріткі салудың, жүйені істен шығарудың, АЖ-ға кірудің және ақпаратқа рұқсатсыз қол жеткізудің негізгі ықтимал жолдары:

1) жүйенің физикалық бұзылуы (жарылыс, өртеу және т. б. жолымен) немесе компьютерлік жүйенің барлық немесе жекелеген аса маңызды компоненттерінің (құрылғылардың, маңызды жүйелік ақпарат тасығыштардың, персонал қатарындағы адамдардың және т. б.) істен шығуы;

2) есептеу жүйелерінің жұмыс істеуін қамтамасыз ететін кіші жүйелерді (электрмен қоректендіру, салқындату және желдету, байланыс желілері және т. б.) ажырату немесе істен шығару;

3) жүйенің жұмыс істеуіне іріткі салу жөніндегі іс-әрекеттер (құрылғылардың немесе бағдарламалардың жұмыс режимдерін өзгерту, персоналдың ереуілі, диверсиясы, жүйе құрылғыларының жұмыс жиіліктерінде қуатты белсенді радиокедергілерді қою және т. б);

4) агенттерді жүйе персоналы қатарына енгізу (оның ішінде, мүмкін, қауіпсіздікке жауап беретін әкімшілік топқа енгізу);

5) персоналды немесе белгілі бір өкілеттіктері бар жекелеген пайдаланушыларды азғырып тарту (сатып алу, бопсалау және т. б. жолымен);

6) тыңдайтын құрылғыларды қолдану, Қашықтықтан фото және бейне түсіру және т. б.;

7) байланыс құрылғылары мен желілерінің жанама электромагниттік, акустикалық және басқа да сәулеленулерін ұстап қалу, сондай-ақ ақпаратты өңдеуге тікелей

қатыспайтын қосалқы техникалық құралдарға (телефон желілері, қоректендіру, жылыту селдері және т. б.) белсенді сәулеленулерді дәлдеу;

8) байланыс арналары арқылы берілетін деректерді ұстап алу және алмасу хаттамаларын, байланысқа кіру және пайдаланушыны авторизациялау қағидаларын және жүйеге кіру үшін оларды имитациялаудың кейінгі әрекеттерін анықтау мақсатында оларды талдау;

9) ақпарат тасымалдағыштарды (магниттік дискілерді, таспаларды, жад микросхемаларын, есте сақтау құрылғыларын және тұтас компьютерлерді) ұрлау;

10) ақпарат жеткізгіштерді санкциясыз көшіруге жол берілмейді;

11) өндірістік қалдықтарды ұрлау (басып шығару, жазбалар, есептен шығарылған ақпарат тасығыштар және т. б.);

12) жедел жадтан және сыртқы сақтау құрылғыларынан қалған ақпаратты оқу;

13) асинхронды режимде Операциялық жүйе (оның ішінде қорғау кіші жүйесі) немесе басқа пайдаланушылар пайдаланатын жедел жады аймақтарынан ақпаратты мультизадачты операциялық жүйелер мен бағдарламалау жүйелерінің кемшіліктерін пайдалана отырып оқу;

14) кейіннен тіркелген пайдаланушы ретінде бүркемелей отырып ("маскарад") парольдерді және қол жеткізуді шектеудің басқа да деректемелерін заңсыз алу (пайдаланушылардың немқұрайлылығын пайдалана отырып, Агенттік жолмен, іріктеу жолымен, жүйе интерфейсін имитациялау жолымен және т. б.);

15) желідегі жұмыс станциясының нөмірі, нақты мекенжайы, байланыс жүйесіндегі мекенжайы, кодтаудың аппараттық блогы және т. б. сияқты бірегей физикалық сипаттамалары бар пайдаланушылар терминалдарын санкцияланбаған пайдалану жатады.;

16) ақпаратты криптографиялық қорғау шифрларын ашу;

17) аппараттық "арнайы салымдарды", бағдарламалық "бетбелгілерді" және "вирустарды" ("трояндық жылқыларды" және "қоңыздарды"), яғни мәлімделген функцияларды жүзеге асыру үшін қажет емес, бірақ қорғау жүйесін еңсеруге, сындарлы ақпаратты тіркеу және беру немесе жүйенің жұмыс істеуіне іріткі салу мақсатында жүйелік ресурстарға жасырын және заңсыз қол жеткізуді жүзеге асыруға мүмкіндік беретін бағдарламалар учаскелерін енгізу;

18) кейіннен жалған хабарламалар енгізе немесе берілетін хабарларды түрлендіре отырып, заңды пайдаланушының өз атынан әрекет етуіндегі үзілістерді пайдалана отырып, "жолдар арасында" жұмыс істеу мақсатында байланыс желілеріне заңсыз қосылу;

19) жүйеге кіргеннен және сәтті аутентификациядан кейін кейіннен дезинформация енгізіп және жалған хабарламалар таңып, заңды пайдаланушыны физикалық ажырату арқылы оны тікелей ауыстыру мақсатында байланыс желілеріне заңсыз қосылу.

Айта кету керек, көбінесе шабуылдаушы мақсатқа жету үшін біреуін емес, жоғарыда аталған жолдардың кейбір жиынтығын пайдаланады.

3. ДАҒДАРЫСТЫҚ ЖАҒДАЙЛАР

Қорғау құралдарымен алдын алмаған АЖ-ға жағымсыз әсер ету нәтижесінде туындайтын жағдай дағдарыс деп аталады.

Дағдарыстық жағдай қаскүнемдік ниеттен немесе кездейсоқ (абайсызда жасалған әрекеттер, авариялар, дүлей зілзалалар және т.б. нәтижесінде) туындауы мүмкін.

Келтірілген залалдың ауырлығы мен мөлшері бойынша дағдарыстық жағдайлар мынадай санаттарға бөлінеді:

Қауіп төндіретін - АЖ-ның толық істен шығуына және оның бұдан әрі өз функцияларын орындай алмауына, сондай-ақ аса маңызды ақпаратты жоюға, бұғаттауға, заңсыз түрлендіруге немесе жария етуге әкеп соғатын;

Елеулі - жүйенің жекелеген компоненттерінің істен шығуына (жұмыс қабілеттілігін ішінара жоғалтуға), өнімділіктің жоғалуына, сондай-ақ санкцияланбаған қол жеткізу нәтижесінде бағдарламалар мен деректердің тұтастығы мен құпиялылығының бұзылуына алып келеді.

Елеулі залал келтірмейтін жағымсыз әсерлер нәтижесінде туындайтын, бірақ соған қарамастан назар аударуды және барабар реакцияны талап ететін жағдайлар (мысалы, жүйенің ресурстарына енудің немесе рұқсатсыз қол жеткізудің тіркелген сәтсіз әрекеттері) сыни жағдайларға жатпайды.

Мысалы, қауіпті дағдарыстық жағдайларға жатқызуға болады:

1) ғимаратқа электр энергиясын беруді бұзу;
2) сервердің істен шығуы (ақпараттың жоғалуымен);
3) сервердің істен шығуы (ақпаратты жоғалтпай);
4) сервердегі ақпараттың жұмыс қабілеттілігін жоғалтпай ішінара жоғалуы;
5) локальдық желінің (деректерді берудің физикалық ортасының) істен шығуы.

Күрделі дағдарыстық жағдайларға, мысалы, жатқызуға болады:

1. жұмыс станциясының істен шығуы (ақпараттың жоғалуымен);
2. жұмыс станциясының істен шығуы (ақпаратты жоғалтпай);
3. жұмыс станциясында жұмыс қабілеттілігін жоғалтпай ақпараттың ішінара жоғалуы;

Назар аударуды қажет ететін жағдайлар, мысалы, мыналарды қамтуы мүмкін:

- қорғау құралдарымен бұғатталған және тіркеу құралдарымен бекітілген рұқсат етілмеген әрекеттер.
- Дағдарыстық жағдайдың туындауы туралы ақпарат көздері:
- жауапкершілік аймағында жүйенің немесе оның қорғаныс құралдарының жұмысында немесе конфигурациясында қорғаныс жоспарына сәйкессіздіктерді немесе басқа күдікті өзгерістерді анықтаған пайдаланушылар;
- қорғаныс жоспарында қарастырылған дағдарыстық жағдайды анықтаған қорғаныс құралдары;
- дағдарыстық жағдайдың туындауын немесе туындау мүмкіндігін куәландыратын жазбалары бар жүйелік журналдар.

4. АЖ ҮЗДІКСІЗ ЖҰМЫСЫН ЖӘНЕ ЖҰМЫС ҚАБІЛЕТТІЛІГІН ҚАЛПЫНА КЕЛТІРУДІ ҚАМТАМАСЫЗ ЕТУ ШАРАЛАРЫ

АЖ жұмыс істеу процесінің үздіксіздігі және оның жұмысқа қабілеттілігін қалпына келтірудің уақтылығына қол жеткізіледі:

1. компьютерді қолдана отырып ақпаратты өңдеу процесін және жүйе қызметкерлерінің әрекеттерін, оның ішінде дағдарыс жағдайларында қатаң реттеу;
2. АЖ есептеу техникасы құралдарын пайдаланатын барлық лауазымды тұлғалардың басшылық құжаттардың талаптарын қатаң сақтауы және нақты білуі;
3. аппараттық ресурстарды резервтеудің әртүрлі тәсілдерін қолдану, жүйенің ақпараттық ресурстарын бағдарламалық және сақтандыру көшірмелерін эталондық көшіру;
4. жүйе құрауыштарының қорғалуының қажетті деңгейін тұрақты ұстап тұру, қорғау құралдарын дұрыс қолдануды үздіксіз басқару және әкімшілік қолдау;

5. қабылданған шаралардың және қорғауды қамтамасыз етудің қолданылатын тәсілдері мен құралдарының тиімділігіне тұрақты талдау жүргізу, оларды жетілдіру жөніндегі ұсыныстарды әзірлеу және іске асыру.

5. ЖАЛПЫ ТАЛАПТАР

Қауіпті немесе күрделі дағдарыстық жағдайдың туындауы нәтижесінде жұмысы бұзылуы мүмкін барлық пайдаланушылар дереу хабардар етілуі тиіс. АЖ жұмыс қабілеттілігінің бұзылу себептерін жою, бүлінген (жоғалған) ресурстарды өңдеуді жаңарту және қалпына келтіру жөніндегі одан арғы іс-қимылдар жүйе персоналы мен пайдаланушыларының функционалдық міндеттерімен айқындалады.

Әрбір дағдарыстық жағдайды қауіпсіздік әкімшілігі талдауы керек және осы талдау нәтижелері бойынша пайдаланушылардың өкілеттіктерін, ресурстарға қол жеткізу атрибуттарын өзгерту, қосымша резервтер құру, жүйенің конфигурациясын немесе қорғаныс құралдарын баптау параметрлерін өзгерту және т. б. ұсыныстар жасалуы керек.

Күрделі және қауіпті дағдарыстық жағдай істен шыққан жабдықты жедел ауыстыруды және жөндеуді, сондай-ақ резервтік көшірмелерден зақымдалған бағдарламалар мен деректер жиынтығын қалпына келтіруді талап етуі мүмкін.

Бағдарламаларды (эталондық көшірмелерді пайдалана отырып) және деректерді (сақтандыру көшірмелерін пайдалана отырып) олар жойылған немесе күрделі немесе қауіпті дағдарыс жағдайында бүлінген жағдайда жедел қалпына келтіру резервтік (сақтандыру) көшірумен және көшірмелерді сыртқы (жүйенің негізгі компоненттеріне қатысты) сақтаумен қамтамасыз етіледі.

Резервтік көшіруге жүйенің жұмыс қабілеттілігін және оның өз міндеттерін орындауын қамтамасыз ететін барлық бағдарламалар мен деректер (жүйелік және қолданбалы бағдарламалық қамтылым, дерекқорлар және басқа да деректер жиынтығы), сондай-ақ мұрағаттар, транзакциялар журналдары, жүйелік журналдар және т. б. жатады.

Жүйеде пайдаланылатын барлық бағдарламалық құралдардың эталондық (дистрибутивтік) көшірмелері болуы тиіс. Олардың орналасқан жері және оларды құруға, сақтауға және пайдалануға жауапты адамдар туралы мәліметтер әрбір компьютерге (жұмыс станциясына, серверге) арналған формулярларда көрсетілуге тиіс. Сондай-ақ, сақтандыру көшірмесін жасауға жататын мәліметтер жиынтығының тізімі, көшіру жиілігі, сақтау орны және деректердің сақтандыру көшірмелерін жасауға, сақтауға және пайдалануға жауапты адамдар көрсетілуі керек.

Бағдарламалар мен деректердің резервтік көшірмелерін жасау, сақтау және пайдалану жөніндегі персоналдың қажетті іс-қимылы персоналдың тиісті санаттарының функционалдық міндеттерінде көрсетілуге тиіс.

Резервтік көшірмені қамтитын әрбір тасығышта сақталатын ақпараттың сыныбы, құндылығы, мақсаты, жасалуы, сақталуы және пайдаланылуы үшін жауапты, соңғы көшірілген күні, Сақтау орны және т. б. туралы деректері бар белгі болуы тиіс.

Қайталанатын аппараттық ресурстар қауіпті дағдарыс жағдайында барлық немесе жеке аппараттық компоненттер істен шыққан жағдайда жүйенің жұмыс істеуін қамтамасыз етуге арналған.

Қайталанатын ресурстардың саны мен сипаттамалары дағдарыс жағдайының жоспарында көзделген кез келген жүйеде негізгі міндеттерді орындауды қамтамасыз етуі тиіс.

Қауіпті немесе ауыр дағдарыстық жағдайдың салдарын жою, мүмкін, жүйенің бағдарламалық, аппараттық, ақпараттық және басқа зақымдалған компоненттерін толығымен қалпына келтіруді білдіреді.

Кез келген дағдарыстық жағдай туындаған жағдайда оның туындау себептерін тексеру, келтірілген залалды бағалау, кінәлілерді айқындау және тиісті шаралар қабылдау жүргізілуге тиіс.

Дағдарыс жағдайын тергеуді мекеме басшылығы тағайындаған топ жүргізеді. Топты қауіпсіздік әкімшісі басқарады. Топтың қорытындылары тікелей ұйым басшылығына баяндалады.

Егер қауіпті немесе күрделі дағдарыстық жағдайдың себебі қорғаныс пен бақылаудың қатаң шаралары жеткіліксіз болса және залал белгіленген деңгейден асып кетсе, онда бұл жағдай қорғаныс жоспарын және үздіксіз жұмыс пен қалпына келтіруді қамтамасыз ету жоспарын толық қайта қарауға негіз болып табылады.

6. АҚПАРАТТЫҚ ҚАУІПСІЗДІК ИНЦИДЕНТТЕРІН БАСҚАРУ

Ақпараттық қауіпсіздік инциденті (бұдан әрі-инцидент) деп ақпараттық жүйеде жасалатын кез келген заңсыз, шешілмеген (оның ішінде ақ саясатымен) немесе қолайсыз әрекет түсініледі.

Ақпараттық жүйелерге қатысты АҚ-ның инциденті мен әлсіздігі туралы Департаменттің ат-ға және барлық мүдделі тараптарға кепілді хабарлауды қамтамасыз ету мақсатында инцидент және қауіп-қатердің пайда болуы туралы хабарлау бойынша формальды рәсімдер іске асырылуы тиіс. Хабарламаларды тарату үшін түзету шараларын уақтылы қабылдауға кепілдік беретін әдіс таңдалуы керек.

Университет қызметкерлері, оның ішінде үшінші тарап пайдаланушылары хабарлама рәсімдерін білуі тиіс, сондай-ақ ұйым ресурстарының қауіпсіздігіне әсер етуі мүмкін түрлі оқиғалар немесе әлсіз жерлер туралы және олардың басталуы немесе олардың алғышарттары туралы хабарлама жіберу қажет.

Қызметкерлер ақпараттық қауіпсіздік саласындағы кез келген оқиғалар туралы тиісті бөлімшеге немесе тікелей ат департаментіне мүмкіндігінше тез хабарлауға міндетті.

7. ИНЦИДЕНТ ТУРАЛЫ ХАБАРЛАУ ФАКТІСІ БОЙЫНША ІС-ҚИМЫЛДАРДЫҢ ЖАЛПЫ СЦЕНАРИЙІ

Оқиғаға жауап беру

Хабарлама тіркелгеннен кейін ат департаменті келесі мақсаттарға жету үшін бірқатар әрекеттерді дәйекті орындау түрінде оқиғаға жауап беру процесін бастауы керек:

1. Үйлестірілмеген іс-қимылдардың алдын алу және қысқа мерзімде инцидент туындаған кезде жүйенің жұмыс қабілеттілігін қалпына келтіру.

2. Ақпаратқа және аппараттық-бағдарламалық құралдарға рұқсатсыз қол жеткізу, ресурстар мен компоненттерге деструктивті әсер ету фактілері немесе ақпараттық қауіпсіздікке қауіп төндіретін оқиғалар анықталған жағдайда департаменттің ат қызметкерлері университет басшылығын міндетті түрде хабардар етуі тиіс.

3. АҚ оқиғасын растау немесе жоққа шығару.

4. Болған оқиға туралы егжей-тегжейлі есепті және пайдалы ұсыныстарды ұсыну.

5. Компьютерлік инциденттер туралы нақты ақпаратты жинақтау және сақтау үшін жағдай жасау.

6. Болашақта осындай инциденттерді жылдам анықтауды және/немесе алдын алуды қамтамасыз ету ("өткен сабақтарды" талдау, АҚ саясатын өзгерту, АҚ жүйесін жаңғырту және т.б. арқылы).

7. Болған инцидент дәлелдемелерінің сақталуын және тұтастығын қамтамасыз ету.

8. Құқық бұзушыларға (Жарғыда, өзге де құжатта) көзделген, оқиғаға барабар тәртіптік шараларды қолдану. Егер оны қаскүнем санатына жатқызуға алғышарттар болса, анықталған бұзушыға қарсы азаматтық немесе қылмыстық іс қозғау мүмкіндігі үшін жағдай жасау.

9. Заңмен белгіленген жеке құқықтарды қорғаңыз.

10. Жұмыс тәртібін бұзуды және АТ-жүйесінің деректеріне зақым келтіруді барынша азайту.

11. It жүйесінің құпиялылығын, тұтастығын және қол жетімділігін бұзудың салдарын азайтыңыз.

12. Университеттің беделін және оның ресурстарын қорғаңыз.

13. Оқыс оқиғаға ден қою процесінде, сондай-ақ оның нәтижелері бойынша персоналды қосымша оқытуды жүргізу.

Инцидентке ден қою процесіне қатысушылардың құрамы

АҚ инциденттерін тергеп - тексеру және оларға ден қою-ұйымның көптеген бөлімшелері қызметкерлерінің: кадрлар бөлімінің қызметкерлерінің, заңгерлердің, ат-жүйесінің техникалық сарапшыларының, ақпараттық қауіпсіздік жөніндегі сыртқы консультанттардың, бизнес-менеджерлердің, ақпараттық жүйенің соңғы пайдаланушыларының, ат департаментінің қызметкерлерінің, қауіпсіздік қызметінің қызметкерлерінің және т. б. қатысуын талап ететін күрделі және кешенді процесс.

АҚ инцидентін тергеу жөніндегі комиссия құрылуы тиіс. Бұл комиссия заң және техникалық салалардағы сарапшылар мен консультанттарды қамтуға тиіс.

Оқиғаға жауап беру процесінің негізгі кезеңдері

Компьютерлік қауіпсіздік оқиғасы көбінесе күрделі және көпжақты проблеманың көрінісі болып табылады. Бұл мәселені шешудің дұрыс тәсілі, ең алдымен, оның құрылымдық компоненттерге бөлінуі және әр компоненттің кірісі мен шығысын зерттеу болып табылады.

Оқиғаға жауап беру процесінің негізгі кезеңдері келесідей.

1. АҚ инцидентінің туындау фактісіне дайындық. Компанияны оқиға жағдайына дайындау үшін шаралар қабылдануда (оның салдарын азайту және компанияның жұмысын тез қалпына келтіру үшін).

2. Инциденттерді тексеру жөніндегі комиссияны құру. Бұл кезең ең маңыздыларының бірі болып табылады, ықтимал оқиғаны тергеудегі сәттілік оған байланысты.

3. Инцидентті анықтау-АҚ инцидентін анықтау.

4. Бастапқы ден қою-бастапқы тергеп-тексеруді жүргізу, оқыс оқиғаға ілесіп жүретін оқиғалардың негізгі бөлшектерін жазу, тергеп-тексеру жөніндегі комиссияны жинау және болған оқиға туралы білуге тиіс адамдарды хабардар ету.

5. Заңсыз әрекеттердің жолын кесу.

6. Әрекет ету стратегиясын қалыптастыру. Стратегия барлық белгілі фактілерге негізделген және оқиғаға жауап берудің ең жақсы жолын анықтайды. Басшылық растайды. Стратегия сондай-ақ инцидент туындауының болжамды себептері мен салдарларына байланысты инциденттің туындау фактісі (азаматтық немесе қылмыстық іс қозғау, әкімшілік ықпал ету) бойынша қандай іс-қимылдар қолданылатынын айқындайды.

7. Инцидентті тергеу-деректерді жинау және талдау арқылы жүргізіледі. Жиналған барлық мәліметтер не болғандығы, қашан болғандығы, қолайсыз әрекеттерді кім жасағаны және болашақта мұның бәрі қалай ескертілетіні туралы тексеріледі.

8. Есеп-тергеу барысында алынған ақпаратты қамтитын егжей-тегжейлі есеп. Шешім қабылдауға ыңғайлы нысанда ұсынылады.

9. Шешім-қорғаныс механизмдерін қолдану және АҚ рәсімдеріне өзгерістер енгізу, "алынған сабақтарды" жазу.

Инцидентті тергеу

Тергеу кезеңі: оқиғаға кім, не, қашан, қайда, қалай және неге қатысқанын анықтауға арналған. Тергеу серверлерден, желілік құрылғылардан дәлелдемелерді тексеруді және жинауды, сондай-ақ техникалық емес сипаттағы дәстүрлі іс-шараларды қамтиды. Ол мүмкін екі сатымен жүргізіледі:

1. деректер жинау;
2. жиналған деректерді сот-медициналық талдау.

Тергеудің бірінші кезеңін орындау барысында жиналған ақпарат одан әрі оқиғаға жауап беру стратегиясын әзірлеу үшін қызмет етеді.

Талдау кезеңінде іс жүзінде оқиғаға кім, не, қалай, қашан, қайда және неге қатысқандығы анықталады.

Жиналған деректерді талдау жүйелік журналдарды, жұмыс хаттамаларының файлдарын, конфигурациялық файлдарды, Интернетке қол жеткізуге арналған қосымшалар тарихын (cookies-ті қоса алғанда), электрондық пошта хабарламаларын және тіркелген файлдарды, орнатылған қосымшаларды, графикалық файлдарды және басқаларды талдауды қамтиды.

Бағдарламалық жасақтаманы талдау, кілт сөздерді іздеу, оқиғаның күні мен уақытын тексеру қажет. Сот-медициналық сараптамаға "төмен" деңгейдегі талдау кіруі мүмкін - жойылған файлдар мен аймақтарды, жоғалған кластерлерді, бос орынды іздеу, сондай-ақ жойылған медиадан қалпына келтірілген деректерді талдау (мысалы, қалдық магниттелу арқылы).

8. АҚПАРАТТЫҚ ҚАУІПСІЗДІК ИНЦИДЕНТТЕРІН БАСҚАРУ РӘСІМДЕРІ

Ақпараттық қауіпсіздік оқиғасы туралы хабарлама

Ақпараттық қауіпсіздік оқиғалары туралы мәліметтер басқарудың тиісті арналары арқылы мүмкіндігінше тез берілуі тиіс.

Ақпараттық қауіпсіздік оқиғалары туралы хабарлама алғаннан кейін қабылданатын іс-қимылдар сипатталған инцидентке ден қою және қауіпсіздік жүйесін жұмылдыру рәсімімен бірге пайдаланылатын ақпараттық қауіпсіздік оқиғалары туралы хабарлаудың формальды рәсімі іске асырылуға тиіс.

Ақпараттық қауіпсіздік оқиғалары туралы хабарлау үшін осындай жағдайда байланысу қажет бөлім анықталуы керек. Осы бөлімшенің шеңберінде хабарламаларды қабылдау мен өңдеудің тұрақты қолжетімді пункті, ерекше жағдайларда - тұрақты жұмыс істейтін АҚ бекеті ұйымдастырылуы тиіс. Пункттің (бекеттің) кезекші персоналының ұйымның барлық ерекшеліктерін ескере отырып, ақ мәселелері бойынша жеткілікті білім деңгейі болуы, барабар және уақтылы жауап беруді қамтамасыз етуі тиіс.

Хабарламаларды беру тетігі туралы мәліметтерді (телефон нөмірі, басқа да тәсілдер) барлық персоналға жеткізу жөнінде шаралар қабылдануға тиіс. Хабарламаларды физикалық түрде беру үшін Сіз IT құрылымының жалпы желісінің мүмкіндіктеріне ғана сенбеуіңіз керек, өйткені ол қазіргі уақытта істен шығуы мүмкін. Пункт нөмірі үшін телефон байланысын пайдаланған кезде қысқартылған теруді, сондай-ақ көп арналы

желіні пайдалану ұсынылады. Ақ пунктінің (бекетінің) нөмірін ұйымның авариялық қызметтері телефондарының тізіміне енгізу қадала ұсынылады.

Ұйым қызметшілерінің, контрагенттердің және үшінші тарап пайдаланушыларының барлық санаттарының лауазымдық нұсқаулықтарында немесе бірдей күші бар өзге де құжаттарда міндеттердің бірі ретінде ақпараттық қауіпсіздіктің кез келген оқиғалары туралы көрсетілген телефон (орын) бойынша мүмкіндігінше тезірек хабарлау міндеті және оны орындау рәсімі көрсетілуге тиіс.

Хабарлама рәсімдері мыналарды қамтуы тиіс:

1. хабарлама көзінің міндетті түрде инцидентке ден қою немесе проблеманы шешу нәтижелерімен танысуына кепілдік беретін кері ақпараттық байланыстың тиісті тізбектері;
2. ақпараттық қауіпсіздік оқиғалары туралы хабарламаны (мысалы, үлгілік мәтін шаблоны бар "хабарлама" түріндегі құжат түрінде), сондай-ақ хабарламаны беру жөніндегі іс-қимылдарды олардың логикалық кезектілігімен (5-9 тармақ) аударатын, ең аз қажетті көлемдегі жадынама түріндегі нұсқаулықты (жеңіл оқылатын қаріппен мәтіннің бір парағы) ұсыну нысандары);
3. ақпараттық қауіпсіздік оқиғасы болған жағдайда персоналдың жеке мінез-құлқы мен іс-қимыл тәртібі Нұсқаулық түрінде, мысалы, осындай мәтінмен:
4. оқиғаның сыртқы көрінісінің барлық мүмкін бөлшектерін бекітіңіз (мысалы, интерфейстің өзгеруі, дисплей мәселелері, біртүрлі жұмыс режимдері, белгісіз хабарламалар, сыртқы байланысты орнатуға өздігінен әрекет жасау…);
5. компьютерді ортақ желіден оқшаулаңыз, сымды желілік картадан немесе байланыс розеткасынан ажыратыңыз
6. АҚ пунктіне (постына) хабарлама қалыптастыру және жіберу
7. өз бастамасы бойынша ешқандай әрекет жасамау және АТ департаменті қызметкерінің келуін немесе ақ пунктінен (бекетінен) хабарлама күтпеу;
8. жеке қауіпсіздікке қауіп төнген жағдайда жағдай бойынша әрекет ету

Персоналдың мәжбүрлі түрде болуы мүмкін жоғары тәуекелдер жағдайындағы іс-қимылдар жалпы қауіпсіздік қызметі немесе сыртқы құзыретті органдар өкілдерінің қатысуымен жасалған арнайы нұсқаулықта көрсетілуге тиіс.

9. АҚПАРАТТЫҚ ҚАУІПСІЗДІК ИНЦИДЕНТТЕРІН ЗЕРДЕЛЕУ

Инциденттерді зерделеу кезінде келтірілген залалдардың түрлеріне, көлемі мен құнына сандық бағалау және мониторинг жүргізілуі тиіс.

Ақпараттық қауіпсіздік инциденттерін бағалау кезінде алынған ақпарат олардың қайталану немесе неғұрлым ауыр салдары бар инциденттердің туындау мүмкіндігін айқындау үшін пайдаланылуға тиіс.

АҚ инциденттерін зерделеудің және олардың алдын алу, анықтау, жою және болдырмау жөніндегі шараларды әзірлеудің нәтижелілігі мен тиімділігі жүргізілген тексерулердің нәтижелері бойынша қалыптастырылатын деректер базасын пайдалану кезінде айтарлықтай артады.

Мұндай база оқиғаның негізгі компоненттерін қамтуы керек: кім, не, қашан, қайда, қалай және неге.

Дәлелдемелер жинау

Инциденттерді тергеу барысында жиналған барлық дәлелдемелер, олардың тәртіптік шаралар кезінде қолданылатынына немесе сот талқылауы процесінде

қолданылатынына қарамастан, жиналуға және қамтамасыз ететін жалпы ережелерге сәйкес сақталуға тиіс:

1. дәлелдеменің жарамдылығы: дәлелдеме шынымен сотта қолданылуы мүмкін бе;
2. дәлелдеменің салмағы: дәлелдеменің сапасы мен толықтығы.

"Дәлелдеменің жарамдылығы" және "дәлелдеменің салмағы" анықтамаларын ұйымның Құзыретті құрылымдары ашады.

Сот мүддесі үшін кез-келген жұмыс тек дәлелдемелер материалдарының көшірмелерімен орындалуы керек.

Барлық дәлелдемелер материалының тұтастығы қорғалуы керек.

Дәлелдемелер материалдарын көшіруді сенімді қызметкерлер бақылауы керек, келесі ақпарат бар есеп жасалуы керек: көшіру процесі қайда және қашан орындалды, көшіру операцияларын кім орындады, қандай құралдар мен бағдарламалар қолданылды, медиа туралы мәліметтер (жеткізуші/өндіруші, түрі, тасымалдаушының зауыттық нөмірі).

IT Департаментінің отырысында қаралды және қабылданды, "28" 01 2020 жылғы №3 хаттама.

КЕЛІСІЛДІ

Оқу-әдістемелік ісі жөніндегі вице-президенті: **Ө.Умбетов**

Құқықтық қамтамасыз ету бөлімінің басшысы: **Г.Мусаханов**

Стратегиялық жоспарлау, рейтинг және сапа орталығының басшысы: **Ж.Дарибаев**

Қосымша А

Ф-СМБ-004

ТАНЫСУ ПАРАҒЫ

№	Аты-жөні	Қызметі	Мерзімі	Қолы