ЛЕКЦИЯ 9
Осалдықтарды анықтау және енуге тестілеудің теориялық негіздері

Лекция мақсаты

Осалдық, қауіп, тәуекел және енуге тестілеу ұғымдарының өзара байланысын ашу; осалдықтарды жіктеу мен анықтау тәсілдерін теориялық тұрғыдан талдау; енуге тестілеудің модельдері мен кезеңдерін, тәуекелді бағалау, есеп беру және қайта тестілеу қағидаларын практикалық мысалдармен түсіндіру.

Негізгі ұғымдар

Актив — ұйым үшін құндылығы бар ақпарат, жүйе, сервис, құрылғы немесе бизнес-функция. ***Қауіп*** — активке зиян келтіруі ықтимал әрекет немесе жағдай. Осалдық — қауіп пайдалана алатын әлсіздік. ***Тәуекел*** — қауіптің осалдықты пайдалану ықтималдығы мен ықтимал салдардың үйлесімі. ***Енуге тестілеу*** — осы әлсіздіктердің нақты қауіпсіздік әсерін келісілген шекарада практикалық бағалау.

Осалдық ұғымы және оның киберқауіпсіздіктегі орны

Осалдық — ақпараттық жүйенің, бағдарламалық қамтамасыз етудің, желілік инфрақұрылымның, конфигурацияның немесе ұйымдастырушылық процестің қауіп көзі пайдалана алатын әлсіз қасиеті. Осалдықтың болуы жүйеге міндетті түрде шабуыл жасалды дегенді білдірмейді. Ол шабуылдың іске асуына мүмкіндік беретін алғышарт болып табылады. Сондықтан осалдықты талдау кезінде оның техникалық сипаты ғана емес, қай активте орналасқаны, сол активтің маңыздылығы, сыртқы ортадан қолжетімділігі және бар қорғаныс механизмдері ескеріледі.

Осалдық ұғымы «қауіп» және «тәуекел» ұғымдарымен тығыз байланысты. Қауіп — активке зиян келтіруі мүмкін жағдай немесе әрекет, ал тәуекел — қауіптің нақты осалдықты пайдалану ықтималдығы мен ықтимал салдардың үйлесімі. Осы себепті бірдей осалдық әртүрлі жүйелерде бірдей тәуекел туғызбайды. Мысалы, Интернетке тікелей ашық өндірістік сервердегі осалдық оқшауланған оқу стендіндегі дәл сондай осалдыққа қарағанда жоғары басымдыққа ие болуы мүмкін.

Практикалық мысал. Ұйымның веб-серверінде ескірген бағдарламалық компонент анықталды делік. Ескірген компонент — осалдық. Оны пайдалануға бағытталған әрекет — қауіп. Егер серверде маңызды деректер сақталса және ол Интернеттен қолжетімді болса, ықтимал салдар жоғары болады. Демек, тәуекелді бағалау кезінде «осалдық бар» деген факт жеткіліксіз; актив пен контекст міндетті түрде ескеріледі.

Осалдықтардың негізгі жіктелуі

Осалдықтарды шығу тегіне қарай бірнеше топқа бөлуге болады. Бағдарламалық осалдықтар бағдарламалық кодтағы логикалық немесе техникалық қателерден пайда болады. Конфигурациялық осалдықтар жүйе дұрыс бапталмаған жағдайда туындайды. Архитектуралық осалдықтар компоненттердің өзара байланысы, сенім шекаралары немесе сегментация дұрыс жобаланбаған кезде қалыптасады. Ұйымдастырушылық осалдықтар құқықтарды басқару, жаңарту, резервтік көшіру, пароль саясаты немесе инциденттерге әрекет ету процестерінің әлсіздігімен байланысты.

Бұл жіктеу қорғаныс шарасын дұрыс таңдауға мүмкіндік береді. Бағдарламалық осалдық көбіне кодты түзету немесе жаңарту арқылы жойылады. Конфигурациялық осалдық баптауды өзгерту арқылы түзетіледі. Архитектуралық мәселе сегментацияны, сенім моделін немесе компоненттердің байланысын қайта қарауды талап етуі мүмкін. Ұйымдастырушылық әлсіздік техникалық құралмен ғана шешілмейді, оған регламент, жауапкершілік және бақылау рәсімдерін өзгерту қажет.

Практикалық мысал. Әдепкі әкімшілік парольдің сақталуы — конфигурациялық осалдық. Пайдаланушы енгізуін дұрыс тексермеу — бағдарламалық осалдық. Маңызды серверлердің пайдаланушы құрылғыларымен бір желілік сегментте орналасуы — архитектуралық әлсіздік.

Жұмыстан шыққан қызметкердің есептік жазбасын уақытында бұғаттамау — ұйымдастырушылық осалдық.

Осалдықтарды анықтау процесі

Осалдықтарды анықтау активтерді түгендеуден басталады. Ұйым қандай серверлер, жұмыс станциялары, желілік құрылғылар, веб-қосымшалар, деректер қорлары және бұлттық ресурстар бар екенін нақты білуі тиіс. Актив туралы ақпарат толық болмаса, сканерлеу мен талдау да толық болмайды. Бұдан кейін операциялық жүйе, бағдарламалық компоненттер, нұсқалар, ашық сервистер және конфигурациялар анықталады.

Автоматтандырылған сканерлер белгілі осалдықтар туралы ақпаратпен салыстырып, ықтимал мәселелерді көрсетеді. Алайда сканер нәтижесі соңғы шешім болып саналмайды. Құрал нұсқаны қате анықтауы, патчтың орнатылғанын ескермеуі немесе нақты конфигурацияны дұрыс түсінбеуі мүмкін. Сондықтан автоматты нәтиже қолмен тексеріліп, контекстпен нақтыланады. Бұл жалған оң нәтижелерді азайтады.

Практикалық мысал. Сканер сервердегі кітапхана нұсқасын осал деп көрсетті. Әкімші тексергенде қауіпсіздік түзетуі сол нұсқаға бөлек backport ретінде енгізілгені анықталды. Демек, бастапқы автоматты белгі нақты осалдықты білдірмеді. Керісінше, сканер ескертуі расталса, активтің маңыздылығы мен сыртқы қолжетімділігі бойынша басымдық беріледі.

Енуге тестілеу ұғымы, мақсаты және шекарасы

Енуге тестілеу — алдын ала берілген жазбаша рұқсат пен нақты келісілген шекара аясында ақпараттық жүйенің қорғанысын практикалық бағалау процесі. Оның негізгі мақсаты жүйеге зиян келтіру емес, анықталған әлсіздіктің нақты қауіпсіздік әсерін растау, қорғаныс механизмдерінің жеткіліктілігін бағалау және түзету бойынша негізделген ұсыным беру.

Енуге тестілеуде scope ұғымы ерекше маңызды. Scope тестіленетін IP-мекенжайларды, домендерді, қосымшаларды, уақыт аралығын, рұқсат етілген және тыйым салынған әрекеттерді анықтайды. Тестілеуші осы шекарадан шықпауы тиіс. Өндірістік жүйелерге әсер етуі мүмкін әрекеттер үшін бөлек келісім мен қауіпсіздік шаралары қажет.

Практикалық мысал. Ұйым тек тест ортасындағы веб-қосымшаны тексеруге рұқсат берді делік. Өндірістік деректер қорын немесе басқа домендерді тексеру техникалық тұрғыдан мүмкін болғанымен, ол келісілген scope құрамына кірмейді және орындалмауы тиіс. Бұл енуге тестілеудің техникалық қана емес, ұйымдастырушылық және құқықтық процесс екенін көрсетеді.

Енуге тестілеудің Black-box, Gray-box және White-box модельдері

Енуге тестілеу тестілеушіге берілетін бастапқы ақпарат көлеміне қарай Black-box, Gray-box және White-box модельдеріне бөлінеді. Black-box моделінде тестілеуші жүйе туралы өте аз ақпарат алады және сыртқы субъектінің бастапқы жағдайына жақын сценарийді модельдейді. Бұл тәсіл сыртқы шабуыл бетін бағалауға пайдалы, бірақ ішкі логиканы толық қамтымауы мүмкін.

Gray-box моделінде тестілеушіге шектеулі ақпарат, мысалы, қарапайым пайдаланушы есептік жазбасы немесе архитектураның бір бөлігі беріледі. Бұл тәсіл аутентификацияланған пайдаланушының мүмкіндіктерін, рөлдер арасындағы шекараны және ішкі функцияларды тексеруге қолайлы. White-box моделінде бастапқы код, архитектура, конфигурация және техникалық құжаттама қолжетімді болады. Ол терең талдауға мүмкіндік береді, бірақ сыртқы шабуылшының нақты бастапқы жағдайын толық модельдемейді.

Практикалық мысал. Интернеттен көрінетін сервистерді бағалау үшін Black-box тәсілі таңдалуы мүмкін. Пайдаланушы рөлдерінің авторизациясын тексеру үшін Gray-box тиімді. Қауіпсіздікке маңызды жаңа қолданбаның кодын, архитектурасын және конфигурациясын кешенді тексеру үшін White-box тәсілі қолданылады.

Енуге тестілеудің негізгі кезеңдері

Енуге тестілеу бір реттік сканерлеу емес, бірнеше өзара байланысты кезеңнен тұратын процесс. Алдымен мақсат, scope, жауапты тұлғалар, байланыс арналары және тоқтату шарттары анықталады.

Одан кейін ақпарат жинау және барлау жүргізіледі. Келесі кезеңде желілік хосттар, порттар, сервистер және қолданбаның кіру нүктелері зерттеледі. Осы деректер негізінде ықтимал осалдықтар анықталып, қауіпсіз түрде расталады.

Растау кезеңінің мақсаты — жүйеге барынша әсер ету емес, осалдықтың шынайылығын және ықтимал салдарын жеткілікті деңгейде дәлелдеу. Бұдан кейін тәуекел бағаланып, есеп дайындалады. Есеп техникалық маманға да, шешім қабылдайтын тұлғаға да түсінікті болуы керек. Соңғы кезең — түзетулер енгізілгеннен кейін қайта тестілеу.

Практикалық мысал. Егер ақпарат жинау кезінде маңызды API анықталмаса, кейінгі тестілеу сол интерфейсті қамтымайды. Егер сканер нәтижесі расталмай есепке енгізілсе, команда жалған мәселені түзетуге уақыт жұмсауы мүмкін. Сондықтан әр кезеңнің сапасы келесі кезеңге тікелей әсер етеді.

Осалдықтарды тәуекел бойынша бағалау және басымдық беру

Осалдықтарды басқаруда барлық анықталған мәселелерді бір уақытта түзету мүмкін бола бермейді. Сондықтан басымдық беру қажет. Техникалық ауырлық — маңызды көрсеткіш, бірақ ол жалғыз критерий емес. Активтің бизнес-маңыздылығы, сыртқы қолжетімділігі, пайдаланылу ықтималдығы, деректердің сезімталдығы және бар қорғаныс қабаттары бірге бағаланады.

Тәуекелге негізделген тәсіл ұйым ресурстарын ең маңызды мәселелерге бағыттауға мүмкіндік береді. Мысалы, орташа техникалық ауырлығы бар, бірақ Интернетке ашық және критикалық сервиске әсер ететін осалдық кейде жоғары техникалық бағасы бар, алайда оқшауланған тест жүйесіндегі осалдықтан бұрын түзетіледі.

Практикалық мысал. Бір осалдық екі серверден табылды: біріншісі — сыртқы клиенттер қолданатын портал, екіншісі — зертханалық ішкі сервер. Осалдық идентификаторы бірдей болғанымен, активтердің маңызы мен қолжетімділігі әртүрлі болғандықтан, remediation басымдығы да әртүрлі болады.

Есеп беру, түзету және қайта тестілеу

Енуге тестілеудің нәтижесі түсінікті және тексерілетін есеппен аяқталады. Әр мәселе үшін осалдықтың атауы, әсер ететін актив, анықталған белгі, ықтимал салдар, тәуекел деңгейі және түзету ұсынымы беріледі. Есепте артық техникалық детальдан гөрі шешім қабылдауға жеткілікті дәлел мен контекст болуы маңызды.

Түзету шаралары мәселенің түріне қарай әртүрлі: бағдарламаны жаңарту, конфигурацияны өзгерту, қажетсіз сервисті өшіру, желілік қолжетімділікті шектеу, құқықтарды қайта бөлу немесе архитектураны өзгерту. Түзетуден кейін қайта тестілеу жүргізіледі. Оның мақсаты — бастапқы мәселенің шынымен жойылғанын және өзгеріс жаңа қауіпсіздік мәселесін тудырмағанын тексеру.

Практикалық мысал. Тестілеу нәтижесінде сыртқы әкімшілік интерфейс анықталды. Ұйым оны VPN арқылы ғана қолжетімді етті. Қайта тестілеу кезінде сыртқы желіден интерфейс енді ашылмайтыны, ал заңды әкімшілік қолжетімділік сақталғаны тексеріледі.

Осалдықтар мен тестілеу модельдерінің жіктелуі

Жіктеу белгісі	**Түрі**	**Негізгі ерекшелігі**	**Мысал**
Шығу тегі	Бағдарламалық	Кодтағы әлсіздік	Енгізуді дұрыс өңдемеу
Шығу тегі	Конфигурациялық	Қауіпсіз емес баптау	Әдепкі пароль
Шығу тегі	Архитектуралық	Құрылымдық әлсіздік	Сегментацияның болмауы
Шығу тегі	Ұйымдастырушылық	Процестің әлсіздігі	Құқықтарды кеш жою
Тест моделі	Black-box	Бастапқы ақпарат аз	Сыртқы периметр
Тест моделі	Gray-box	Шектеулі ішкі ақпарат	Пайдаланушы рөлі

Тест моделі	White-box	Толық техникалық ақпарат	Код пен архитектура

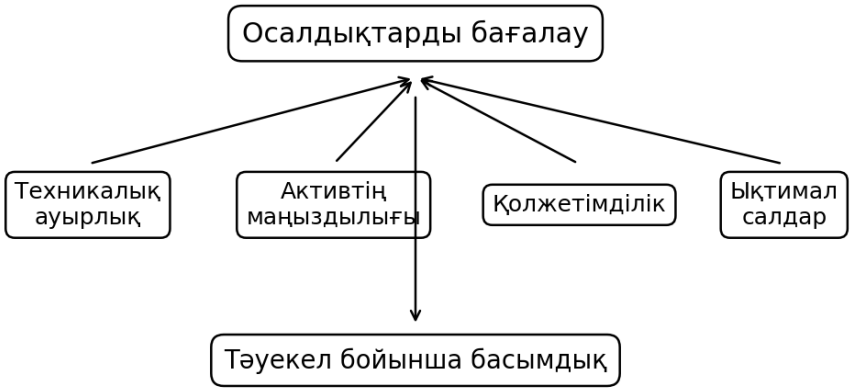
Осалдық, қауіп және тәуекелдің өзара байланысы



Сурет 1. Осалдықтарды анықтау мен басқарудың жалпы логикалық байланысы

Схемада актив бастапқы қорғалатын объект ретінде көрсетілген. Қауіп осалдықпен түйіскен кезде тәуекел қалыптасады. Тестілеу тәуекелдің техникалық негізін тексеруге көмектеседі, ал түзету және қайта тестілеу қорғанысты үздіксіз жетілдіру циклін аяқтайды.

Тәуекелді бағалау факторлары



Сурет 2. Осалдықты тәуекел бойынша басымдыққа қою факторлары

Суреттен көрінгендей, техникалық ауырлық жалғыз фактор емес. Активтің маңыздылығы, сыртқы қолжетімділік және ықтимал салдар бірге қарастырылғанда ғана remediation басымдығы негізді анықталады.

Практикалық кешенді мысал

Ұйымда сыртқы веб-портал, ішкі деректер қоры және тест сервері бар делік. Инвентаризация кезінде веб-порталда ескірген компонент, деректер қорында артық желілік қолжетімділік, ал тест серверінде әдепкі пароль анықталды. Бірінші кезеңде әр мәселе жеке осалдық ретінде тіркеледі. Екінші кезеңде олардың активтермен байланысы қарастырылады. Веб-портал Интернетке ашық және клиенттік деректерді өңдейді; деректер қоры маңызды ақпарат сақтайды; тест сервері оқшауланған. Сондықтан осалдықтарды тек техникалық атауы бойынша емес, контекст бойынша басымдыққа қою қажет.

Енуге тестілеу барысында веб-порталға қатысты осалдық қауіпсіз түрде расталып, оның нақты әсері анықталады. Деректер қорына қатысты мәселе желілік сегментация мен firewall ережелерін талдау арқылы тексеріледі. Тест серверіндегі әдепкі пароль де түзетіледі, бірақ оның басымдығы басқа екі активке қарағанда төмен болуы мүмкін. Түзетулерден кейін қайта тестілеу жүргізіліп, сыртқы экспозицияның азайғаны және заңды бизнес-функциялар сақталғаны тексеріледі.

Артықшылықтары мен шектеулері

Тәсіл	Артықшылығы	Шектеуі

Автоматты сканерлеу	Үлкен инфрақұрылымды жылдам қамтиды	Жалған оң/теріс нәтиже болуы мүмкін
Қолмен талдау	Контекст пен нақты конфигурацияны ескереді	Уақыт пен біліктілік қажет
Енуге тестілеу	Осалдықтың нақты әсерін бағалайды	Scope және қауіпсіздік шектеулері міндетті
Тәуекелге негізделген басымдық	Ресурсты маңызды мәселеге бағыттайды	Актив туралы сапалы дерек қажет
Қайта тестілеу	Түзетуді объективті растайды	Қосымша уақыт қажет

Қорытынды

Осалдықтарды анықтау мен енуге тестілеу киберқауіпсіздіктің өзара байланысты, бірақ бірдей емес процестері. Осалдықтарды анықтау ықтимал әлсіздіктерді табуға бағытталса, енуге тестілеу олардың нақты қауіпсіздік әсерін келісілген шекарада тексеруге мүмкіндік береді. Тәуекелді дұрыс бағалау үшін техникалық белгі активтің маңыздылығымен, сыртқы қолжетімділікпен және ықтимал салдармен бірге қарастырылуы тиіс. Нәтиже есеппен бекітіліп, түзетуден кейін қайта тестілеумен аяқталады.

Бақылау сұрақтары

1. Осалдық, қауіп және тәуекел ұғымдарының айырмашылығын түсіндіріңіз.
2. Осалдықтардың негізгі түрлерін атаңыз және мысал келтіріңіз.
3. Автоматтандырылған сканер нәтижесін неге қолмен растау қажет?
4. Енуге тестілеудің мақсаты қандай?
5. Scope неліктен міндетті түрде алдын ала анықталады?
6. Black-box, Gray-box және White-box модельдерін салыстырыңыз.
7. Енуге тестілеудің негізгі кезеңдерін атаңыз.
8. Осалдыққа басымдық беру кезінде қандай факторлар ескеріледі?
9. Есепте қандай негізгі ақпарат болуы тиіс?
10. Қайта тестілеудің мақсатын түсіндіріңіз.

Әдебиеттер тізімі

1. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение : учебно-методическое пособие. — Санкт-Петербург : Университет ИТМО, 2018. — 45 с.

2. Силлабус SEC247 «Кибершабуылдарды анықтау және оларға қарсы әрекет етудің интеллектуалды құралдары». 9-апта тақырыбы және ұсынылған әдебиеттер.