ДӘРІС 10

Ақпарат жинау, желіні сканерлеу және шабуыл бетін анықтау

Оқытушы: проф. Ахмедиярова А.Т.

Негізгі түсініктер

Негізгі түсініктер

Тақырыптың негізгі ұғымдарына анықтама беру, оларды теориялық тұрғыдан талдау, жіктеу және өзара байланысын практикалық мысалдар арқылы түсіндіру.

Ақпарат жинау

Ақпарат жинау — қорғалатын инфрақұрылым, ақпараттық жүйе, пайдаланушылар, желілік ресурстар және олардың өзара байланыстары туралы техникалық және ұйымдастырушылық деректерді жүйелі түрде алу процесі. Ақпарат жинаудың негізгі мақсаты — қорғалатын ортаның нақты құрылымын анықтау және кейінгі қауіпсіздік талдауы үшін жеткілікті бастапқы деректер қалыптастыру.

Ақпарат жинау

Ақпарат жинау киберқауіпсіздікті қамтамасыз етудің бастапқы кезеңдерінің бірі болып табылады. Қандай ақпараттық ресурстар бар екені белгісіз болса, олардың барлығын бақылау және қорғау мүмкін емес. Мысалы, ұйымда ресми есепке алынбаған сервер, веб-қосымша немесе желілік құрылғы болуы мүмкін. Мұндай объектілер жаңартылмауы, журналдары бақыланбауы және қауіпсіздік саясатына енгізілмеуі мүмкін.

Ақпарат жинау

Ақпарат жинау

Сондықтан оларды кейде «көлеңкелі активтер» (shadow assets) деп атайды.

Ақпарат жинау қалай жүзеге асырылады?

Алдымен зерттелетін объект және ақпарат жинаудың шекарасы анықталады. Одан кейін активтер туралы қолда бар құжаттар, желінің құрылымы, серверлер, жұмыс станциялары, пайдаланушылар, бағдарламалық қамтамасыз ету, желілік сервистер және сыртқы ресурстар туралы мәліметтер жиналады. Алынған ақпарат салыстырылып, қайталанатын немесе ескірген деректер алынып тасталады.

Ақпарат жинау қалай жүзеге асырылады?

Соңында ұйымның нақты ақпараттық инфрақұрылымының сипаттамасы қалыптастырылады. Ақпаратты жинау барысында, мысалы, мынадай мәліметтер анықталуы мүмкін: сервердің IP-мекенжайы, операциялық жүйесі, іске қосылған сервистері, пайдаланылатын бағдарламалар, домендік атаулар, желілік құрылғылар, пайдаланушылардың рөлдері, сыртқы ақпараттық жүйелермен байланыстары және деректердің қандай түрлері өңделетіні.

Ақпарат жинау қалай жүзеге асырылады?

Ақпарат жинау қалай жүзеге асырылады?

Ақпарат жинаудың ерекшелігі — деректердің бір ғана көзден алынбауында. Бір дереккөз жүйенің толық жағдайын көрсете алмайды. Мысалы, ұйымның техникалық құжаттамасында сервер көрсетілгенімен, нақты желіде ол жұмыс істемеуі мүмкін. Керісінше, құжатта жоқ жаңа сервер желіде белсенді болуы мүмкін. Сондықтан құжаттық мәліметтер нақты техникалық жағдаймен салыстырылуы қажет.

Ақпарат жинау қалай жүзеге асырылады?

Ақпарат жинау пассивті және белсенді түрде жүзеге асырылуы мүмкін. Пассивті жинауда зерттелетін жүйеге тікелей әсер етпей, бұрыннан бар құжаттар, активтер реестрі, журналдар және қолжетімді метадеректер зерттеледі. Белсенді жинауда рұқсат етілген инфрақұрылымға тікелей сұраныстар жіберіліп, белсенді құрылғылар, порттар мен сервистер анықталады.

Ақпарат жинау қалай жүзеге асырылады?

Белсенді әдістер нақты әрі өзекті ақпарат береді, бірақ олар желіде тіркеледі және өндірістік жүйелерге артық жүктеме түсірмеуі тиіс.

Ақпарат жинағанда нені ескеру қажет?

Ақпарат жинағанда нені ескеру қажет?

Ең алдымен жиналатын ақпараттың мақсаты мен көлемі анықталуы керек. Қажетсіз деректерді жинау дұрыс емес. Сонымен қатар ақпараттың құпиялылығы, тұтастығы, өзектілігі және заңды түрде өңделуі ескеріледі. Әсіресе жеке тұлғалар туралы мәліметтермен жұмыс істегенде бұл талаптар маңызды. Мысалы, тұрғындар туралы ақпарат жиналатын ақпараттық жүйені қарастырайық.

Ақпарат жинағанда нені ескеру қажет?

Жүйеде адамның аты-жөні, туған күні, мекенжайы, байланыс деректері және басқа да жеке мәліметтер болуы мүмкін. Киберқауіпсіздік маманына шабуыл бетін анықтау үшін барлық тұрғындардың нақты жеке мәліметтерін көшірудің қажеті жоқ. Оның орнына қандай деректер сақталатыны, олар қай серверде орналасқаны, кімнің оларға қолжетімділігі бар, қандай ақпараттық жүйелермен алмасатыны және қандай қорғау құралдары қолданылатыны анықталады.

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Осы тізбекті талдау барысында әрбір байланыс жеке бақылау нүктесі ретінде қарастырылады. Егер тұрғындардың деректер қоры Интернеттен тікелей қолжетімді болмаса, бірақ оған веб-қосымша арқылы сұраныс жасалса, онда веб-қосымша мен оның API интерфейстері шабуыл бетінің маңызды бөлігіне айналады. Тағы бір мысал: тұрғындардың деректеріне тек операторлар қол жеткізуі тиіс делік.

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Ақпарат жинау кезінде жүйеде бұрын жұмыс істеген қызметкерлердің белсенді есептік жазбалары сақталғаны анықталса, бұл жай ғана «пайдаланушылар тізімі» емес, қолжетімділікті басқарудағы ықтимал қауіпсіздік мәселесі болып табылады. Осылайша, ақпарат жинаудың нәтижесі жай ғана IP-мекенжайлар немесе пайдаланушылар тізімі болмауы керек.

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Оның нәтижесінде қандай актив қорғалады, онда қандай ақпарат өңделеді, оған кім және қандай жолмен қол жеткізеді, қандай сыртқы байланыстар бар және қай жерде ықтимал шабуыл беті қалыптасады деген сұрақтарға жауап алынуы тиіс. Пассивті ақпарат жинау — зерттелетін ақпараттық жүйеге немесе желіге тікелей сұраныс жібермей, ол туралы мәліметтерді қолда бар дереккөздерден алу процесі.

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Мұндай дереккөздерге ұйымның техникалық құжаттамасы, активтер реестрі, желі схемалары, домендер туралы мәліметтер, бұрын қалыптасқан журналдар және басқа метадеректер жатады. Пассивті жинаудың негізгі ерекшелігі — зерттелетін жүйенің жұмысына тікелей әсер етпеуі. Сондықтан бұл тәсіл қауіпсіз және бастапқы талдау үшін қолайлы. Алайда алынған ақпарат ескірген немесе толық емес болуы мүмкін.

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Мысалы, желі схемасында көрсетілген сервер іс жүзінде пайдаланылмауы мүмкін немесе керісінше, жақында орнатылған жаңа сервер құжаттамаға әлі енгізілмеген болуы мүмкін. Белсенді ақпарат жинау — зерттелетін желімен немесе ақпараттық жүйемен тікелей өзара әрекеттесу арқылы нақты техникалық мәліметтерді анықтау процесі.

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Белсенді жинау кезінде рұқсат етілген желі диапазоны тексеріліп, жұмыс істеп тұрған хосттар, ашық порттар, желілік сервистер және олардың кейбір сипаттамалары анықталады. Белсенді жинаудың артықшылығы — жүйенің нақты ағымдағы жағдайын көрсетуі. Бірақ мұндай әрекеттер желілік журналдарда тіркелуі мүмкін және кейбір жағдайларда ақпараттық жүйеге қосымша жүктеме түсіреді.

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Сондықтан белсенді жинау тек алдын ала белгіленген шекарада және тиісті рұқсатпен жүргізілуі тиіс. Пассивті және белсенді жинау бір-бірін алмастырмайды, керісінше бірін-бірі толықтырады. Пассивті әдістер жүйе туралы бастапқы түсінік қалыптастырса, белсенді әдістер сол ақпараттың нақты жағдайға сәйкестігін тексеруге мүмкіндік береді. Мысал. Тұрғындар туралы ақпарат сақталатын ақпараттық жүйені тексеру қажет делік.

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Пассивті жинау кезінде жүйенің архитектуралық схемасы, серверлер тізімі, деректер қорының орналасуы, пайдаланушылардың рөлдері және сыртқы ақпараттық жүйелермен байланыстары зерттеледі. Құжат бойынша жүйеде веб-сервер, қолданбалар сервері және деректер қорының сервері бар екені анықталуы мүмкін. Белсенді жинау кезінде рұқсат етілген желі диапазоны тексеріліп, нақты жұмыс істеп тұрған серверлер мен сервистер анықталады.

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Нәтижесінде құжаттамада көрсетілмеген қосымша сервер немесе қажетсіз ашық сервис табылуы мүмкін. Мұндай айырмашылық қауіпсіздік тұрғысынан маңызды, себебі есепке алынбаған актив жаңартылмай немесе тиісті мониторингпен қамтылмай қалуы ықтимал. Сондықтан ақпарат жинаудың нәтижесінде «құжат бойынша жүйе қандай?» және «нақты жағдайда жүйе қандай?» деген екі сұрақтың жауабы салыстырылуы тиіс.

Тұрғындар туралы деректер → деректер қоры → веб-қосымша → API → сыртқы мемлекеттік жүйе

Осы салыстыру кейінгі желіні сканерлеу, шабуыл бетін анықтау және осалдықтарды бағалау кезеңдеріне негіз болады.

Желіні сканерлеу

Желіні сканерлеу

Желіні сканерлеу — желіге қосылған белсенді құрылғыларды, олардың IP-мекенжайларын, ашық порттарын және жұмыс істейтін желілік сервистерін анықтау процесі. Ол ақпарат жинаудың белсенді әдістерінің бірі болып табылады және ұйымның желілік инфрақұрылымының нақты ағымдағы жағдайын анықтауға мүмкіндік береді. Желіні сканерлеу кезінде алдымен берілген желі диапазонында қандай хосттар белсенді екені анықталады.

Желіні сканерлеу

Хост ретінде сервер, жұмыс станциясы, маршрутизатор, желілік принтер, бейнебақылау құрылғысы немесе басқа желілік құрылғы болуы мүмкін. Одан кейін белсенді хосттардағы ашық порттар және сол порттар арқылы жұмыс істейтін сервистер зерттеледі.

Желіні сканерлеу

Желіні сканерлеу әдетте мынадай логикалық ретпен жүзеге асырылады: Желі диапазоны → Белсенді хосттар → Ашық порттар → Сервистер → Нұсқалар мен конфигурациялар → Қауіпсіздік тұрғысынан бағалау Сканерлеудің маңызды ерекшелігі — ашық порт немесе жұмыс істейтін сервис автоматты түрде осалдық болып саналмайды. Мысалы, веб-серверде веб-қызмет көрсетуге арналған порттың ашық болуы қалыпты жағдай.

Желіні сканерлеу

Желіні сканерлеу

Бірақ сол серверде ұйым пайдаланбайтын қашықтан басқару сервисі ашық тұрса, ол шабуыл бетін негізсіз кеңейтеді. Сондықтан сканерлеу нәтижесін талдағанда бірнеше сұраққа жауап беру қажет: бұл сервис не үшін қажет, оны кім пайдаланады, оған қай желілерден қол жеткізуге болады, сервис жаңартылған ба, аутентификация қалай ұйымдастырылған және оның жұмыс істеуі ұйымның қауіпсіздік саясатына сәйкес келе ме?

Желіні сканерлеу

Желіні сканерлеудің тағы бір маңызды міндеті — активтер реестрін нақтылау. Құжаттамада көрсетілген құрылғылар нақты желідегі құрылғылармен салыстырылады. Нәтижесінде құжатта жоқ серверлер, бұрын пайдаланылған, бірақ әлі де желіге қосылған құрылғылар немесе есепке алынбаған сервистер анықталуы мүмкін. Мысал. Тұрғындар туралы ақпарат сақталатын ақпараттық жүйенің желісін қарастырайық.

Желіні сканерлеу

Құжаттама бойынша жүйеде веб-сервер, қолданбалар сервері және деректер қоры сервері бар делік. Желіні сканерлеу нәтижесінде осы үш сервермен қатар бұрын тестілеу үшін пайдаланылған төртінші сервердің де әлі жұмыс істеп тұрғаны анықталды. Тест серверінде тұрғындардың нақты деректері сақталмауы мүмкін. Бірақ онда негізгі жүйемен бірдей бағдарламалық қамтамасыз ету орнатылған және қашықтан басқару сервисі ашық болуы ықтимал.

Желіні сканерлеу

Желіні сканерлеу

Егер бұл сервер жаңартылмаса немесе мониторинг жүйесіне қосылмаса, ол ұйымның есепке алынбаған шабуыл бетіне айналады. Сонымен бірге деректер қоры серверінің порты бүкіл ішкі желіге ашық екені анықталды делік. Деректер қорымен шын мәнінде тек қолданбалар сервері жұмыс істеуі керек болса, мұндай кең қолжетімділік қажет емес.

Пайдаланушы → Веб-сервер → Қолданбалар сервері → Деректер қоры

Ал пайдаланушы компьютерлерінен деректер қорына тікелей қосылуға қажеттілік жоқ. Сондықтан желілік сегментация және firewall ережелері арқылы деректер қоры серверіне тек қажетті жүйелерден қолжетімділік беріледі. Осылайша, желіні сканерлеудің мақсаты тек ашық порттардың тізімін алу емес.

Пайдаланушы → Веб-сервер → Қолданбалар сервері → Деректер қоры

Оның нәтижесінде нақты желілік құрылым анықталып, құжаттамамен салыстырылады, қажетсіз сервистер мен артық қолжетімділік табылады және олардың шабуыл бетіне әсері бағаланады. Бұл ақпарат кейінгі осалдықтарды анықтау және енуге тестілеу кезеңдерінің негізін құрайды.

Порт және сервис

Порт және сервис

Порт — желідегі құрылғыда белгілі бір қолданбаға немесе желілік қызметке келетін және одан шығатын деректер ағынын ажыратуға арналған логикалық байланыс нүктесі. Порт нөмірі операциялық жүйеге келген желілік трафикті тиісті сервиске бағыттауға мүмкіндік береді. Сервис — желі арқылы пайдаланушыларға, құрылғыларға немесе басқа ақпараттық жүйелерге белгілі бір функция ұсынатын бағдарламалық қызмет.

Порт және сервис

Мысалы, веб-сервис веб-беттер мен API-ге қолжетімділікті қамтамасыз етеді, деректер қоры сервисі ақпаратты сақтау мен өңдеуді жүзеге асырады, ал электрондық пошта сервисі хабарламаларды қабылдау және жіберу үшін қолданылады. Порт пен сервис өзара байланысты болғанымен, олар бір ұғым емес:

Клиент → IP-мекенжай → Порт → Сервис → Қолданба немесе ресурс

Яғни IP-мекенжай қажетті құрылғыны, порт сол құрылғыдағы байланыс нүктесін, ал сервис қандай қызмет көрсетілетінін анықтайды.

Кең таралған сервистердің мысалдары

Кең таралған сервистердің мысалдары

Киберқауіпсіздік тұрғысынан ашық порттың болуы автоматты түрде осалдық бар дегенді білдірмейді. Егер порт арқылы жұмыс істейтін сервис ұйымға қажет болса, дұрыс конфигурацияланған, жаңартылған және оған қолжетімділік тиісті түрде шектелген болса, оның жұмыс істеуі қалыпты жағдай. Сондықтан порт пен сервисті талдау кезінде «порт ашық па?» деген сұрақпен шектелуге болмайды.

Кең таралған сервистердің мысалдары

Келесі мәселелер анықталуы қажет: қандай сервис жұмыс істейді, ол не үшін қажет, қандай нұсқасы орнатылған, кімдер оған қол жеткізе алады, аутентификация қалай орындалады және сервис қандай активке қолжетімділік береді? Мысалы, ұйымның веб-серверінде 443-порттың ашық болуы қалыпты, себебі пайдаланушылар веб-қосымшаға HTTPS арқылы қосылады.

Кең таралған сервистердің мысалдары

Бірақ дәл сол серверде әкімшілік басқаруға арналған сервис Интернеттен барлық пайдаланушыларға қолжетімді болса, шабуыл беті негізсіз кеңейеді. Мұндай жағдайда әкімшілік сервисті тек ішкі желіден немесе қорғалған VPN арқылы қолжетімді ету дұрыс шешім болуы мүмкін. Сервистің нұсқасы да маңызды. Бір портта әртүрлі бағдарламалық өнімдер мен олардың әртүрлі нұсқалары жұмыс істей алады.

Кең таралған сервистердің мысалдары

Кең таралған сервистердің мысалдары

Егер сервис ұзақ уақыт жаңартылмаса, онда белгілі осалдықтар болуы ықтимал. Сондықтан желіні сканерлеуден алынған порттар тізімі кейін сервистерді, олардың нұсқаларын және конфигурацияларын талдаумен толықтырылады. Сервис конфигурациясы жеке қарастырылады. Бағдарламаның соңғы нұсқасы қолданылғанымен, қауіпсіз емес баптаулар тәуекел туғызуы мүмкін.

Кең таралған сервистердің мысалдары

Мысалы, қажетсіз функциялардың қосулы болуы, әлсіз аутентификация, тым кең желілік қолжетімділік немесе артық пайдаланушы құқықтары сервистің қауіпсіздік деңгейін төмендетеді. Мысал. Тұрғындар туралы ақпарат сақталатын жүйеде мына архитектура бар делік:

Пайдаланушы → 443-порт → Веб-сервис → Қолданбалар сервері → Деректер қоры

Пайдаланушыларға веб-сервис қажет болғандықтан, 443-порт сырттан қолжетімді болуы заңды. Бірақ тұрғындардың жеке деректері орналасқан деректер қоры серверінің сервисі Интернеттен тікелей қолжетімді болмауы тиіс. Онымен тек қолданбалар сервері байланысуы қажет.

Интернет → Деректер қоры — бұғатталады

Интернет → Деректер қоры — бұғатталады

Егер сканерлеу барысында деректер қорының сервисі сыртқы желіден тікелей қолжетімді екені анықталса, мәселе тек «ашық портта» емес. Негізгі мәселе — маңызды активке қажетсіз тікелей қолжетімділіктің пайда болуы. Осылайша, порт пен сервисті бағалауда олардың бар-жоғын анықтау жеткіліксіз.

Интернет → Деректер қоры — бұғатталады

Сервистің қажеттілігі, бағдарламалық нұсқасы, конфигурациясы, оған қол жеткізетін субъектілер, желілік орналасуы және қорғалатын активтің маңыздылығы бірге қарастырылуы тиіс. Осындай талдау қажетсіз сервистерді анықтауға, қолжетімділікті шектеуге және ақпараттық жүйенің жалпы шабуыл бетін азайтуға мүмкіндік береді.

Шабуыл беті

Шабуыл беті (Attack Surface) — ақпараттық жүйеге сыртқы немесе ішкі субъект әсер ете алатын барлық интерфейстердің, кіру нүктелерінің, сервистердің және сенім байланыстарының жиынтығы. Оған веб-интерфейстер, API, VPN, электрондық пошта, қашықтан басқару сервистері, мобильді қосымшалар, бұлттық сервистер және үшінші тарап жүйелерімен интеграциялар кіреді. Шабуыл беті тек Интернетке ашық сервистерден тұрмайды.

Шабуыл беті

Шабуыл беті

Оның құрамына сыртқы, ішкі және пайдаланушымен байланысты компоненттер де кіреді. Мысалы, ұйымның ішкі желісіндегі әкімшілік панель Интернеттен көрінбеуі мүмкін, бірақ оған ішкі пайдаланушының есептік жазбасы арқылы қол жеткізуге болатындықтан, ол да жалпы шабуыл бетінің бөлігі болып табылады. Шабуыл бетін анықтағанда алдымен ұйымның активтері түгенделеді, содан кейін әр активке қандай жолмен қол жеткізуге болатыны анықталады.

Шабуыл беті

Әрбір веб-интерфейс, API, ашық порт, пайдаланушы тіркелгісі немесе сыртқы интеграция жеке кіру нүктесі ретінде қарастырылады. Шабуыл бетінің маңызды ерекшелігі — оның тұрақты болмауы. Ақпараттық жүйеге жаңа сервис, API, мобильді қосымша немесе бұлттық компонент қосылған сайын шабуыл беті де өзгереді. Сондықтан оны бір рет анықтап қою жеткіліксіз; жүйедегі өзгерістерге сәйкес үнемі қайта бағалау қажет. Мысал.

Шабуыл беті

Тұрғындар туралы ақпарат сақталатын жүйеде пайдаланушылар веб-портал арқылы қызмет алады делік. Портал мобильді қосымшамен, ішкі деректер қорымен және басқа мемлекеттік жүйенің API-імен байланысады. Пайдаланушы → Веб-портал → API → Деректер қоры Мобильді қосымша → API → Деректер қоры Сыртқы жүйе → Интеграциялық API → Ақпараттық жүйе Бұл жағдайда тек веб-порталды қорғау жеткіліксіз.

Шабуыл беті

Шабуыл беті

API, мобильді қосымша, сыртқы интеграция және оларға берілген қолжетімділік құқықтары да шабуыл бетіне кіреді. Бір интерфейстің қорғанысы әлсіз болса, ол арқылы маңызды деректерге жанама қолжетімділік пайда болуы мүмкін.

Шабуыл векторы

Шабуыл векторы (Attack Vector) — қауіп субъектісінің ақпараттық жүйеге кіру, оған әсер ету немесе қорғалатын ресурсқа қол жеткізу үшін пайдалануы ықтимал жолы немесе тәсілі. Шабуыл беті мен шабуыл векторы бір ұғым емес. Шабуыл беті жүйеде қай жерлерге әсер етуге болатынын, ал шабуыл векторы сол нүктелердің қалай пайдаланылуы мүмкін екенін сипаттайды.

Мысалы

Веб-портал — шабуыл бетінің элементі. Веб-порталдағы әлсіз аутентификацияны пайдалану — ықтимал шабуыл векторы. Шабуыл векторлары техникалық қана емес, пайдаланушылармен және ұйымдастырушылық процестермен де байланысты болуы мүмкін. Шабуыл векторын бағалау кезінде оның бар-жоғын ғана емес, іске асу ықтималдығын және қандай активке алып келетінін анықтау қажет.

Мысалы

Мысалы

Маңызды деректерге тікелей немесе жанама жол ашатын векторлар бірінші кезекте қарастырылады. Мысал. Тұрғындар туралы ақпараттық жүйеге кіру үшін операторлар логин мен пароль пайдаланады делік. Оператордың есептік жазбасы — қолжетімділік механизмі, ал сол есептік жазбаны фишинг арқылы иемдену — ықтимал шабуыл векторы.

Мысалы

Егер бір есептік жазба арқылы тұрғындардың үлкен көлемдегі деректеріне қол жеткізуге мүмкіндік берілсе, ықтимал салдар жоғары болады.

Сенім шекарасы

Сенім шекарасы (Trust Boundary) — ақпараттық жүйеде бір қауіпсіздік деңгейінен немесе сенім аймағынан екіншісіне өту жүзеге асатын логикалық немесе физикалық шекара. Мысалы, Интернеттен ұйымның желісіне өту, DMZ аймағынан ішкі желіге өту, қарапайым пайдаланушы құқықтарынан әкімшілік құқықтарға ауысу — сенім шекаралары болып табылады.

Сенім шекарасы

Сенім шекарасы

Сенім шекарасынан өткен кезде жүйе субъектіні немесе деректі автоматты түрде сенімді деп қабылдамауы тиіс. Сондықтан мұндай нүктелерде аутентификация, авторизация, желілік сүзу, шифрлау және журналдау сияқты бақылаулар қолданылады.

Интернет ↔ DMZ — сенімсіз сыртқы ортадан ұйым бақылайтын аймаққа өту;

DMZ ↔ Ішкі желі — сырттан қолжетімді серверлер орналасқан аймақтан маңызды ішкі ресурстарға өту. Сенім шекарасының негізгі мақсаты — шабуылшы бір компонентке қол жеткізген жағдайда оның басқа жүйелерге еркін таралуына жол бермеу. Мысал. Тұрғындар туралы ақпараттық жүйенің веб-сервері DMZ аймағында, ал деректер қоры ішкі қорғалған желіде орналассын.

Интернет → Веб-сервер (DMZ) → Қолданбалар сервері → Деректер қоры

Егер веб-серверде қауіпсіздік мәселесі пайда болса, ол деректер қорына толық желілік қолжетімділік бермеуі тиіс. Firewall ережелері тек қажетті қолданбалар серверінен және қажетті сервис бойынша байланысқа рұқсат береді. Осылайша, сенім шекарасы тек желіні физикалық бөлу емес. Ол қай субъект қандай ресурсқа, қандай жағдайда және қандай құқықпен өте алатынын анықтайтын қауіпсіздік бақылауының нүктесі болып табылады.

Шабуыл бетін азайту — Attack Surface Reduction

Шабуыл бетін азайту — Attack Surface Reduction

Attack Surface Reduction (ASR) — ақпараттық жүйеде шабуыл үшін пайдаланылуы мүмкін қажетсіз кіру нүктелерін, сервистерді, функцияларды және артық құқықтарды жүйелі түрде азайту процесі. ASR-дың негізгі қағидасы өте қарапайым: пайдаланылмайтын функция шабуылшы үшін де қолжетімді болмауы керек.

Шабуыл бетін азайту — Attack Surface Reduction

Сондықтан ұйымға қажет емес сервистерді өшіру, сыртқы қолжетімділікті шектеу, пайдаланушыларға ең аз құқық беру, желіні сегменттеу және бағдарламалық қамтамасыз етуді жаңарту шабуыл бетін азайтады. Шабуыл бетін азайту бірнеше бағытта жүзеге асырылады: ASR жүргізген кезде барлық сервисті жай ғана жабу дұрыс емес. Алдымен олардың бизнес-процеске қажеттілігі анықталады. Қауіпсіздік шарасы жүйенің негізгі қызметін тоқтатпауы тиіс.

Шабуыл бетін азайту — Attack Surface Reduction

Сондықтан шабуыл бетін азайту қауіпсіздік пен функционалдықтың теңгеріміне негізделеді. Мысал. Тұрғындар туралы ақпараттық жүйеде 50 оператор жұмыс істейді делік. Талдау барысында жұмыстан кеткен 8 қызметкердің есептік жазбалары әлі белсенді, тест сервері өндірістік желіге қосылған және деректер қорының сервисіне барлық ішкі жұмыс станцияларынан қол жеткізуге болатыны анықталды.

ASR нәтижесінде

ASR нәтижесінде

8 қажетсіз есептік жазба → бұғатталады; тест сервері → оқшауланады; деректер қоры → тек қолданбалар серверіне қолжетімді болады; қажетсіз сервистер → өшіріледі; әкімшілік интерфейс → VPN арқылы ғана қолжетімді болады. Нәтижесінде қорғалатын деректер өзгермейді және жүйенің негізгі қызметі сақталады, бірақ оған жетуге болатын артық жолдардың саны азаяды.

ASR нәтижесінде

Осы төрт ұғымның байланысын былай көрсетуге болады: Актив → Шабуыл беті → Кіру нүктесі → Шабуыл векторы → Сенім шекарасы → Қорғаныс шаралары → Attack Surface Reduction Яғни алдымен нені қорғайтынымыз, содан кейін оған қандай жолдармен жетуге болатыны, сол жолдардың қалай пайдаланылуы мүмкін екені және оларды қандай шекаралар мен қорғаныс механизмдері арқылы шектеуге болатыны анықталады.

Өзара байланыстар схемасы

Схема бастапқы объектілер мен деректердің талдау кезеңдері арқылы қорғаныс шешіміне қалай өтетінін көрсетеді. Кері байланыс нәтижелері алдыңғы кезеңдерді нақтылауға және қауіпсіздік шараларын үздіксіз жетілдіруге мүмкіндік береді.

Практикалық мысал

Практикалық мысал

Ұйымда қауіпсіздік оқиғасы немесе осалдық белгісі анықталды делік. Алдымен оның қай активке қатысты екені, активтің маңыздылығы және сыртқы қолжетімділігі анықталады. Кейін техникалық белгі басқа дереккөздермен салыстырылады. Егер белгі расталса, ықтимал салдар бағаланып, түзету немесе әрекет ету шарасы таңдалады. Соңында нәтиже қайта тексеріледі.

Практикалық мысал

Бұл мысал техникалық анықтау, тәуекелді бағалау және қорғаныс шешімінің бір-бірінен бөлінбейтінін көрсетеді.

Артықшылықтары мен шектеулері

Кешенді тәсілдің артықшылығы — бір ғана белгіге сүйенбей, бірнеше дереккөз бен әдісті байланыстыру. Бұл жалған қорытынды ықтималдығын азайтады және басымдықты дұрыс анықтауға көмектеседі. Шектеулеріне деректердің толық болмауы, жалған оң және жалған теріс нәтижелер, конфигурация қателері, ресурстық шығын және сарапшының контекстік бағасына қажеттілік жатады.

Қорытынды

Қорытынды

Ақпарат жинау, желіні сканерлеу және шабуыл бетін анықтау кибершабуылдарды анықтау және оларға қарсы әрекет ету циклінің маңызды бөлігі. Тақырыпты меңгеруде ұғымдардың анықтамасын білу жеткіліксіз: олардың өзара байланысын, қолданылу шекарасын, артықшылықтары мен шектеулерін түсіну қажет.

Бақылау сұрақтары

1. Негізгі ұғымдарға анықтама беріңіз. 2. Негізгі жіктеуді түсіндіріңіз. 3. Процестің кезеңдерін атаңыз. 4. Әдістердің айырмашылығы қандай? 5. Артықшылықтары қандай? 6. Шектеулері қандай? 7. Практикалық мысалды талдаңыз. 8. Контекст не үшін қажет? 9. Схемадағы байланысты түсіндіріңіз. 10. Тақырып интеллектуалды киберқорғаныспен қалай байланысады?

Әдебиеттер тізімі

1. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. — СПб.: Университет ИТМО, 2018. 2. Сигалов Д.А. Методы выявления поверхности атаки веб-приложений. — М.: МГУ, 2024.

Негізгі әдістер мен сипаттамаларды салыстыру

Салыстыру белгісі	Пассивті жинау	Белсенді жинау
Жүйемен тікелей әрекет	Жоқ	Бар
Негізгі дереккөз	Құжаттар, реестрлер, схемалар, метадеректер	Хосттар, порттар, сервистер
Ақпараттың өзектілігі	Ескірген болуы мүмкін	Ағымдағы жағдайды көрсетеді
Жүйеге әсері	Өте төмен	Қосымша жүктеме болуы мүмкін
Негізгі мақсаты	Бастапқы ақпарат қалыптастыру	Нақты техникалық жағдайды тексеру

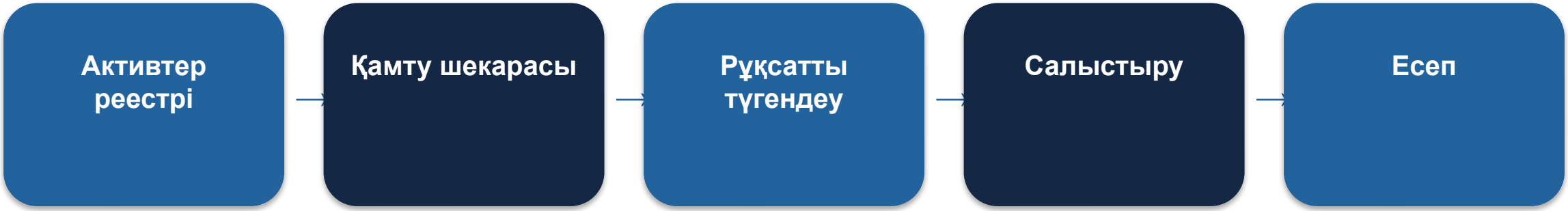
Негізгі әдістер мен сипаттамаларды салыстыру

Сканерлеу объектісі	Нені анықтайды	Қауіпсіздік тұрғысынан маңызы
Хост	Желіде қандай құрылғы белсенді	Есепке алынбаған активтерді анықтау
IP-мекенжай	Құрылғының желідегі орны	Активті нақты сәйкестендіру
Порт	Қандай байланыс нүктелері ашық	Артық экспозицияны анықтау
Сервис	Қандай желілік қызмет жұмыс істейді	Қажеттілігін және қауіпсіздігін бағалау
Сервис нұсқасы	Қолданылатын БҚ нұсқасы	Ескірген компоненттерді анықтауға көмектесу

Негізгі әдістер мен сипаттамаларды салыстыру

Порттар диапазоны	Сипаттамасы	Қолданылуы
0–1023	Жүйелік немесе well-known порттар	Кең таралған стандартты сервистер
1024–49151	Тіркелген порттар	Қолданбалар мен арнайы сервистер
49152–65535	Динамикалық немесе жеке порттар	Уақытша клиенттік байланыстар

Жүйенің жалпы жұмыс істеу архитектурасы



Әр кезеңнің нәтижесі келесі кезеңнің кіріс дерегі болады. Мониторинг пен тексеру нәтижелері қорғаныс шешімін нақтылауға мүмкіндік береді.

Түйінді ұғымдар және қолданылуы

Негізгі түсініктер

Тақырыптың негізгі ұғымдарына анықтама беру, оларды теориялық тұрғыдан талдау, жіктеу және өзара байланысын практикалық мысалдар арқылы түсіндіру.

Ақпарат жинау

Ақпарат жинау — қорғалатын инфрақұрылым, ақпараттық жүйе, пайдаланушылар, желілік ресурстар және олардың өзара байланыстары туралы техникалық және ұйымдастырушылық деректерді жүйелі түрде алу процесі. Ақпарат жинаудың негізгі мақсаты — қорғалатын ортаның нақты құрылымын анықтау және кейінгі қауіпсіз

Ақпарат жинау

Ақпарат жинау киберқауіпсіздікті қамтамасыз етудің бастапқы кезеңдерінің бірі болып табылады. Қандай ақпараттық ресурстар бар екені белгісіз болса, олардың барлығын бақылау және қорғау мүмкін емес. Мысалы, ұйымда ресми есепке алынбаған сервер, веб-қосымша немесе желілік құрылғы болуы мүмкін. Мұндай

Ақпарат жинау

Сондықтан оларды кейде «көлеңкелі активтер» (shadow assets) деп атайды.

Қорытынды және талдау сұрақтары

Негізгі қорытынды

Ақпарат жинау, желіні сканерлеу және шабуыл бетін анықтау. Қорғаныс шешімін қабылдағанда деректер сапасы, жүйенің контексті және тәуекел деңгейі бірге бағаланады.

Талдау тапсырмасы

Берілген жүйе үшін негізгі активтерді, қауіп белгілерін, анықтау әдісін және қорғаныс шараларын бір сызбада көрсетіңіз.

Салыстыру

Қарастырылған тәсілдердің артықшылықтары мен шектеулерін нақты мысал арқылы түсіндіріңіз.