11-семинар сабағы

БАҒДАРЛАМАЛЫҚ ЖАБДЫҚТАУ АУДИТІНІҢ ҚАЖЕТТІЛІГІ МЕН МІНДЕТТЕРІ

Корпоративті сектордағы компаниялар мен мемлекеттік ұйымдар қолданбалы және жүйелік бағдарламалық жасақтаманы — биллинг, ақпараттық банк жүйелері, CRM, ERP, ЭДО, ДҚБЖ, АЖЖ, АБЖ және басқаларын нөлден жасайды немесе нақты талаптарды ескере отырып аяқтайды. Кәсіпорынның қорғалған ақпараты үшін 4 негізгі қауіп осы процеспен байланысты:

Бағдарламалау қателері қосымшалардың қалыпты жұмысына кедергі келтіріп қана қоймайды (қатып қалу, BSOD, деректердің жоғалуы), сонымен қатар шабуылдаушыны оларды пайдалануға "шақырады".

Қауіпсіздікке зиян келтіретін қосымшалардың функционалдығын кеңейту. Әзірлеушілер ең қарапайым (бірақ қауіпсіз емес!) мерзімдері мен ыңғайлылығын қуғындау тәсілдері.

Қорғаныс тетіктерін айналып өтуге мүмкіндік беретін функцияларды ендіру. Бағдарламалық жасақтаманы жасаушылар мұндай функцияларды қосымшаларды тестілеу мен күйін келтіруді жеңілдету үшін қалдырады, бірақ оларды соңғы нұсқада өшіруді ұмытып кетеді.

Қосымшалардың бастапқы кодына немесе БҚ жаңартуларына қасақана енгізілетін және ақпаратқа немесе басқа да зиянды әрекеттерге рұқсатсыз қол жеткізу үшін пайдаланылатын бағдарламалық бетбелгілер. Бетбелгінің бастапқы кодына әзірлеушінің өзі немесе оған шабуыл жасаған шабуылдаушы кіреді.

Бағдарламалық жасақтама аудиті не үшін қажет?

Қосымшаларды өзіңіз жасайсыз ба, әлде оны әзірлеуге тапсырыс бересіз бе, өмірлік циклдің әртүрлі кезеңдерінде бағдарламалық жасақтаманы зерттеу

3 мақсатты көздейді:

1. Қателер немесе бетбелгілері бар бизнес-қосымшаларға шабуылдардан тікелей қаржылық шығындар қаупін азайту.
2. Бағдарламалық жасақтаманы өнеркәсіптік пайдалануға әзірлеу мен енгізуді бақылау арқылы корпоративтік ақпараттық жүйелердің қауіпсіздігін арттыру.

3. Компанияның беделін сақтау. Бастапқы кодта және қосымшаларды пайдалану кезінде қателер неғұрлым аз болса, пайдаланушылардың істен шығу, тоқтап қалу және теріс тәжірибе қаупі соғұрлым аз болады.

Бағдарламалық жабдықтау аудит міндеттері

Әзірленген кодтың осалдықтарын анықтау
"Перспективалық мониторинг" зерттеушілері құрастырылған және бастапқы кодтың осалдықтарын анықтау үшін статикалық және динамикалық талдау әдістерін қолданады. Жұмыс нәтижелері бойынша біз сипаттамасы және сыныптамасы бар анықталған осалдықтардың тізбесін жасаймыз, зиянкес іске асыра алатын табысты шабуылдардың сценарийлерін және осы осалдықтарды жою үшін не істеу керектігін қарау керек.

Бойынша бөгде компоненттердің осалдығын мониторингтеу
Зиянкестер шабуыл жасау үшін БҚ әзірлеу кезінде пайдаланылатын бөгде сервистердің, қызметтер мен кітапханалардың жалпыға мәлім осалдықтарын пайдаланады. Мұндай осалдықтардың жарқын мысалдары — Heartbleed және Shellshock. Бұған жол бермеу үшін анықталған осалдықтар туралы өзекті ақпаратты үнемі жинап, өңдеу қажет. Аудитор Клиентті онлайн режимінде хабардар етіп. және осы түрдегі компьютерлік шабуылдардың алдын алуға көмектеседі.

Жаңарту жүйесінің қауіпсіздігін талдау
Зиянкестің БҚ жаңартуларын ауыстыру мүмкіндіктерін анықтау үшін аудитор жаңартуларды жеткізу мен орнату кезінде іске қосылған инфрақұрылымды және БҚ-ның өзінде іске асырылған жаңартуларды қорғау жөніндегі техникалық шараларды зерттейді. Нәтиже жаңартуларды ауыстыру тәуекелін төмендетуге бағытталған инфрақұрылымды қорғау шаралары мен БҚ түзету бойынша ұсынымдар болып табылады.

Журнал жүргізу жүйесін талдау
Оқиғаларды бақылау және ақпараттық жүйеде инциденттерді тексеру үшін журналдарда толық ақпаратты тіркеу және қауіпсіздік үшін маңызды оқиғалар тізбегін анықтау үшін мониторинг жүйесін орнату

қажет. Егер Тапсырыс беруші бақылау және журнал жүргізу құралдарын орнатпаса, аудитор оны қалай дұрыс жасау керектігі туралы ұсыныстар береді.

БЖ (SDL) қауіпсіз әзірлеу практикасын енгізу)

Қауіпсіздікке зиян келтірместен қосымшалардың қажетті функционалдығын жүзеге асыру және осалдықтарды жою шығындарын азайту үшін өмірлік циклдің барлық кезеңдерінде қауіпсіздікке қатысты бірқатар тексерулер жүргізіледі: талаптарды әзірлеу, сәулет, код, тестілеу, енгізу және пайдалану. "Перспективалық мониторинг" сыртқы сарапшы ретінде осындай тексерулер жүргізеді немесе Тапсырыс берушіде қауіпсіз әзірлеу практикасын енгізуге көмектеседі.