Қайырлы күн, құрметті студенттер! Мен сіздердің барлықтарыңызды кезекті сұрақ-жауап сессиясында көргеніме қуаныштымын. Біз сізді қызықтыратын тағы бір сұрақтар жиынтығын алдық. Осы сессияда біз әр сұрақты егжей-тегжейлі қарастырып, талдаймыз. Сонымен, бастайық.

Сұрақ: “Виртуализация инфрақұрылымы термині нені білдіреді?” Жауап. Жалпы “виртуализация инфрақұрылымы” деген термин жоқ. Бұл өз алдына бөлек екі термин. Инфрақұрылымның не екенін біз талқыладық. Мен сіздерге қазір виртуализацияның не екенін түсіндіремін. Виртуализацияның не екенін түсіндіру үшін дата-центрдің не екенін еске түсірейік. AWS дата-центрі – бұл серверлер орналасқан үлкен ғимарат. Әрбір сервер шкаф түрінде орналасқан, осы шкафтағы әрбір сөреде бөлек серверлер бар. AWS физикалық кеңістікті оңтайлы пайдалану үшін бір шкафта есептеу қуатының барынша көп мөлшерін орналастыруға тырысады. Осылайша осы серверлік шкафтың ішіндегі әрбір сервер біздің ең озық компьютерлер мен ноутбуктерге қарағанда он есе күштірек. Енді ары қарай көрейік. Біз AWS ішінде бірнеше түрлі инстанстарды таңдауға мүмкіндік бар екенін білеміз, яғни сіз ең әлсіз екі гигабайттық жадысы мен бір ядролық процессоры бар инстансты, ары қарай одан күштірек ондаған процессордың қуаты және жүздеген гигабайттық жедел жадысы бар өте қуатты серверді таңдай аласыз. Енді осы сияқты үлкен және кіші серверлерді бөлуге және таңдауға мүмкіндік беру үшін виртуализация технологиясы әзірленді. Бұл нені білдіреді? Бұл қарапайым тілмен айтқанда, өз қуаттылығы бар арнайы физикалық сервер бар екенін білдіреді. Бұл процессорлар саны, сондай-ақ оперативті жады көлемі. Виртуализация бізге бір сервердің осы қуаттылықтарын бөлшектеп, бір-бірінен тәуелсіз бөлек, кішігірім серверлерді виртуалды алуға мүмкіндік береді. Осылайша, біз, мысалы, виртуализация технологиясы арқылы екі процессор және төрт жедел жадысы бар серверді екіге бөле аламыз. Осылайша бір процессордан және екі гигабайт жедел жадысы бар тәуелсіз жұмыс істейтін екі бөлек серверді аласыз. Енді виртуализация инфрақұрылымына оралсақ, бұл жағдайда AWS физикалық серверлерді виртуалдандыру процесін қолдауға, оларды бірнеше кішкене бөліктерге бөлуге және бізге AWS пайдаланушылары ретінде кіші серверден бөлек тұрған өте қуатты серверге дейінгілерді таңдау мүмкіндігін беру.

Сұрақ: “Implicit allow және implicit deny мағыналарын нақты мысалмен түсіндіре аласыз ба?” Жауап беремін. Сіз, ең алдымен, implicit-тің не екенін түсінуіңіз керек. Implicit – бұл басынан бастап, әдепкі ретінде бар жағдай. Сондықтан біз implicit allow десек, бұл әдепкі бойынша рұқсат етілген дегенді білдіреді. Біз implicit deny десек – бұл әдепкі бойынша тыйым салынған дегенді білдіреді. Егер біз AWS туралы айтатын болсақ, онда қол жеткізуге қатысты әрекеттер әдепкі бойынша тыйым салынады. Яғни, тек Implicit deny ғана бар. Implicit allow AWS аясында жоқ. Осылайша, мысал келтіретін болсақ, сіз жаңа пайдаланушыны құрасыз және бұл пайдаланушының тіркелген policy-і жоқ, ол белгілі бір пайдаланушыға inline тіркелген немесе оған бекітілген жеке policy болуы мүмкін. Егер мұның ешқайсысы болмаса, бұл пайдаланушы әдепкі бойынша ешқандай сервиске қол жеткізе алмайды. Себебі, біздің AWS-та implicit deny.

Сұрақ: “Explicit allow және explicit deny мағыналарын нақты мысалмен түсіндіре аласыз ба?” Жауап беремін: біз explicit allow және explicit deny туралы айтатын болсақ біз пайдаланушыға кейбір ресурстарға қандай да бір әрекеттер жасауға нақты рұқсат берілгені немесе оны нақты жасауға тыйым салатыны жазылғандығын білдіреді. Үшінші нұсқа бар – implicit deny. Бұл әдепкі бойынша істелінетін әрекет. Әдепкі бойынша, егер ештеңе нақты көрсетілмесе, онда кіруге рұқсат етілмейді. Енді белгілі бір операцияға және белгілі бір AWS ресурстарға нақты identity-ге қол жеткізу рұқсат етілгенін немесе рұқсат етілмегенін түсіну үшін AWS қандай қадамдар жасайтынын мысал ретінде қарастырайық. Менің пайдаланушым, user Yelzhan бакет ішіндегі объектілердің тізімін, мысалы bucket01, ашқысы келетінін елестетіп көрейік. Бұл жағдайда пайдаланушы user Yelzhan, мен мұнда орындағым келетін операция list objects және осы операция орындалатын ресурс осы bucket01. Яғни, нақты ресурстың ARN-і. Енді AWS қалай жұмыс істейді. Ол осы әрекетті қабылдағаннан кейін, ол explicit deny-дің бар екендігін тексере бастайды. Яғни, белгілі бір әрекетке нақты тыйым салатын кем дегенде бір policy бар ма? Егер explicit deny болса, онда бұл жағдайда explicit allow-дың кез келген саны есепке алынбайды, қол жетімділік берілмейді. Басқа жағдайда, егер AWS explicit deny-ді таппаса, яғни бұл әрекетке нақты тыйым салынбаған, бұл жағдайда ол келесі кезеңге өтеді. Екінші кезең – explicit allow-дің бар екендігін тексеру. Яғни, біздің операциямызға қол жетімділікті нақты қамтамасыз ететін кем дегенде бір policy бар ма? Егер ол сол policy-ді тапса, онда менің пайдаланушыма bucket01 ішіндегі объектілердің тізімін көруге рұқсат етіледі. Егер AWS нақты операцияға қол жетімділікті қамтамасыз ететін policy-ді таппаса, онда нақты операция case осы пайдаланушы үшін policy-дің барлығында тіркелмеген. Бұл жағдайда әдепкі бойынша орнатылған тәртіп іске қосылады; бұл жағдай implicit deny, кіруге рұқсат берілмейді.

Сұрақ: “AWS қаскүнемдердің шабуылына қаншалықты жиі ұшырайды?” Жауап: Дәрісте біз Shared Responsibility Model-дің не екенін талқыладық. Бұл сервисті ұсыну моделіне байланысты, біз, яғни AWS пайдаланушылары, немесе AWS инфрақұрылымның қай бөлігіне жауапты екенін анықтайтын модель. Сервисті ұсыну моделінің үш нұсқаны бар: IaaS – Infrastructure as a service, біз ресурстарды толығымен басқарамыз. PaaS – Platform as a service, бір бөлігі үшін біз жауап беретін болсақ, бір бөлігіне AWS жауап береді. Үшіншіден, SaaS – Software as a service, сервис дайын өнім ретінде ұсынылады және сервис пен қауіпсіздік үшін жауапкершіліктің көп бөлігі AWS жағында болады. Біз ПО сервисті конфигурациялау деңгейінде ғана өзгертіп және қауіпсіздік тұрғысынан осы бөлігі үшін ғана жауаптымыз. Яғни, шабуылдың санын азайту үшін біз бұл сервисті жауапкершілікпен баптауымыз керек. Сервис қандай модель арқылы ұсынылғанына қарамастан, сервер, дата-центрлер, AWS жаһандық инфрақұрылымы да бұлтты провайдердің жауакершілігі. Егер шабуылдардың болуы мүмкін жерлері туралы айтатын болсақ, онда сәйкесінше екіге бөлінеді. Бұл біз жауапты жерлері және AWS жауапты жерлер. Сұрақтан түсінуімше, біз AWS пайдаланушылары ретінде, бұлттағы IT инфрақұрылымды дұрыс баптадық, мүмкіндігінше қауіпсіздендірдік және шабуыл AWS жауапты жерде өткені айтылады. Бұл жағдайда, AWS сапа стандарттарына, нормативтік талаптарға және ережелерге сәйкестікке сертификаттау рәсімдері тұрақты негізде жүргізіліп жатқанын еске түсірген жөн. Берілген барлық сертификаттар AWS Artifact сервисінде жарияланады, бұл жерден сіз осы сертификаттар мен құжаттарды сұраныс бойынша өзіңізге тегін жүктей аласыз. AWS-тің әр түрлі сапа сертификаттарының болуы және әртүрлі нормативтік талаптарға сәйкестігі сізге бірнеше мүмкіндіктер береді. Ең айқын екеуі: бірінші – сізге бұл сертификатты қайта алудың қажеті жоқ, себебі бұл сертификатты сіз үшін AWS алды. Егер сіз өзіңіздің инфрақұрылымыңызды AWS бұлтында орналастырсаңыз, сіз осы сертификаттарды тиісті органдарға сұраныс бойынша бере аласыз және олар жарамды болады. Екіншісі – осы әрбір сертификатты сәтті өту үшін компанияның дайындығына байланысты бірнеше айдан бірнеше жылға дейін уақыт қажет. Осылайша, компания ішінде өткізіліп жатқан көптеген процесстер, компания жұмысының аспектілері өзгереді және ықтимал шабуыл алаңдарының көпшілігі алынып тасталады немесе дұрыс бапталынады және шабуылдың сәтті жүзеге асырылу мүмкіндігі азайтылады. Мұның бәрінен шығатыны, осы сертификаттардың болуы кепілдік пен сенімділікті қамтамасыз етеді, атап айтқанда, бұл сапа сертификаттары жоқ кез-келген басқа компаниялармен салыстырғанда AWS шабуылдарға сирек ұшырайды.

Сұрақ: “Шифрлау кілттері дегеніміз не?” Жауап: сіз өзіңіздің университетіңіздегі қауіпсіздік бойынша жеке дисциплинада шифрлау кілттері туралы көбірек білетін боласыз, мен AWS бұлтында жұмыс істеу үшін білуіңіз керек негізгі ақпаратты ғана түсіндіремін. Қарапайым шифрлау әдісінің мысалын қарастырайық. Бізде «папа» сөзі бар делік және бізге бұл мәтінді шифрлау керек. Біздің шифрлау әдісіміз – алфавит бойынша келесі әріпке ауыстыру. Осылайша, папа сөзінде п – р болады, ал а – б болады. Нәтижесінде – рбрб болып табылатын шифрланған мәтін алдық. Осылайша, сіз шифрлаудың қандай екендігі туралы жалпы түсінік алдыңыз. Бізде кірісте шифрланбаған мәтінді нәтижесінде шифрланған мәтінге айналдыру үшін пайдаланылатын белгілі бір көлемі бар мәтін бар деп айтатын болсақ, бұл мәтінді шифрлау кілті деп айтамыз. Осы шифрлау кілтінің көмегімен сіз шифрланған мәтінді шифрдан шығарып, бастапқы мәтінді оқи аласыз. Бұл кілтсіз, сізде шифрланған мәтін болса да, сіз онымен ештеңе жасай алмайсыз және одан пайдалы ақпарат ала алмайсыз. Сонымен, encryption keys бізде KMS сервисінде кездеседі, Key Management Service, яғни біз шифрлаудың қандай әдістері қолданылатынын және осы шифрлау кілттерін қалай басқаратыны туралы толығырақ сөйлесеміз.

Сұрақ: “Қандай ұйым AWS бұлтты провайдерін немесе жалпы кез-келген бұлт провайдерін сертификаттарға сәйкестігін тексереді?” Жауап: сапа стандарттарына сәйкестік сертификаты немесе белгілі бір нормативтік талаптарға сәйкестік сертификаты болсын, жалпы сертификаттар туралы айтатын болсақ, әрбір сертификаттың негізінде осы талаптарды әзірлеуге және осы сертификатқа мұқтаж компанияларды тексеруге бағытталған компания немесе ұйым тұрады, содан кейін осы сертификат беріледі. Жеке сертификаттың құндылығы сол ұйымның қаншалықты танымал және маңызды екеніне байланысты. Біз AWS туралы айтқан кезде, көбінесе AWS Certified Cloud Practitioner емтиханын айтатын болсақ, үш сертификат жиі атап өтіледі. Бірінші сертификат – HIPAA, соңында екі А. Бұл медицина саласында жұмыс істейтін IT компаниялар үшін сапа стандарттарын белгілейтін сертификат. Екіншісі – бұл GDPR. Бұл Еуропадағы ЕО-қа кіретін пайдаланушылардың, адамдардың жеке деректерінің сақталуын, өңделуін және тасымалдауын реттейтін құжат. Және жиі кездесетін үшіншісі – ISO 27001. Бұл жалпыға белгілі сапа стандарты. Ол компанияның жұмыс істеуінің әртүрлі аспектілеріне байланысты бірнеше түрлі бөлімдерден тұрады, айтарлықтай жалпы болып табылады. Және осы сапа стандартының сертификатымен олар компания ішіндегі процесс жұмысты тиімді жасау үшін дұрыс құрылғанын айтады.

Осымен біз сіздерден келген барлық сұрақтарды қарастырдық. Сіздер жауап алдыңыздар деп үміттенемін. Осымен біз сұрақ-жауап сессиясын аяқтаймыз. Келесі белсенділіктерімізде кездескенше! Сау болыңыздар!