Ақпараттық қауіпсіздік және деректерді қорғау

Ақпараттық қауіпсіздік және деректерді қорғау Қордың бизнес тұрақтылығы мен қызметінің үздіксіздігін қолдайды. Цифрландыру және кибер-қатерлердің өсуі жағдайында Қор ақпараттық активтерді қорғауды қорғаныс архитектурасына, тәуекелдерді басқаруға, ішкі аудитке және қол жеткізу құқықтарын шектеуге қойылатын талаптарды белгілейтін бірыңғай Ақпараттық қауіпсіздіктің корпоративтік стандарты негізінде басқарады.

2025 жылы біз ISO 27001 талаптарын ескере отырып, тәуекелге бағдарланған тәсіл негізінде жүйенің дамуын жалғастырдық. IT-инфрақұрылымды талдау және оңтайландыру, сондай-ақ процестердің қорғалу деңгейі мен кемелдігін бағалау жүргізілді. Нәтижелер бойынша рәсімделген процестер, жауапкершілікті бөлу және ақпараттық қауіпсіздіктің негізгі мәселелері бойынша басшылықты ақпараттандыру жүйесінің жұмыс істеуі расталды.

Инфрақұрылымның қорғалуын қамтамасыз ету бөлігінде IT-жүйелерді тексеру жүргізілді, ықтимал істен шығу нүктелері мен осалдықтар анықталды, OSINT-талдауды қолдана отырып, сыртқы веб-ресурстар оңтайландырылды. Қорғаныс «қара жәшік» моделі бойынша, оның ішінде ішкі инфрақұрылым, ілеспе жүйелер және жұмыскерлердің әлеуметтік-инженерлік әсерлерге төзімділігі бойынша тестіленді.

Орташа және сыни деңгейдегі осалдықтар жойылды; инфрақұрылымды бақылауды бұзуға әкеліп соқтыруы мүмкін елеулі ымыраға келу сценарийлері анықталмаған. Істен шығуға төзімділікті арттыру үшін сервер және желілік жабдықты орналастыру оңтайландырылды, сыни инфрақұрылым үшін гео-резервтеу қамтамасыз етілді, ақпараттық қауіпсіздік оқиғаларын мониторингтеу, ағып кетудің алдын алу және осалдықтарды сканерлеуге арналған заманауи шешімдер енгізілді.

Кибертұрақтылық жүйесінің маңызды элементі — оқиғаларды орталықтандырылған мониторингтеу және оларға ден қою. Кибершабуылдарға қарсы тұру үшін Қор тобында «QazCloud» ЖШС негізінде Қордағы және портфельдік компаниялардағы ақпараттық қауіпсіздік оқиғаларын тәулік бойы мониторингтеуді қамтамасыз ететін «Киберщит» жобасы іске асырылып жатыр.

Қор инфрақұрылымды мамандандырылған лицензияланған бағдарламалық жасақтаманы пайдалана отырып үнемі сканерлейді, тәуекел көздері мен киберқауіпсіздік оқиғаларының тізбесін қалыптастырады, сондай-ақ тәуекелдер бойынша тұрақты есептерді дайындайды.

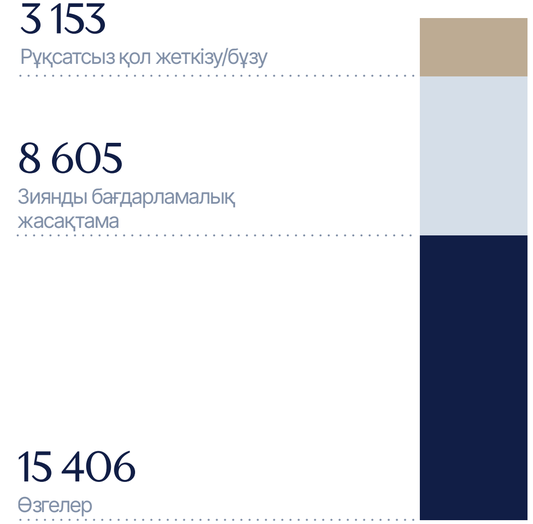
Корпоративтік стандарт аясында портфельдік компаниялар тоқсан сайын инциденттер туралы ақпаратты жібереді, ол компаниялардың өздерінің деңгейінде де, Қор деңгейінде де талданады. Бұл орталықтандырылған бақылауды және ақпараттық жүйелердің құпиялылығына, тұтастығы мен қолжетімділігіне төнетін қатерлерді барынша азайту жөніндегі шараларды уақтылы қабылдауды қамтамасыз етеді.

2025 жыл қорытындысы бойынша Топта 2024 жылмен салыстырғанда 8,05%-ға көп болатын 27 164 инцидент тіркелді. Көрсеткіштің өсуі ең алдымен мониторинг қамтуын кеңейтуге және анықтау жүйелерінің сезімталдығын арттыруға байланысты. Сыни деңгей бойынша төмен және орта деңгейдегі инциденттер басым, бұл ерте сатыда анықталатын оқиғалардың жоғары үлесін көрсетеді.

Инциденттердің негізгішоғырлануы Топтың бірқатар ірі ұйымдарында, оның ішінде «Қазақстан темір жолы» ҰК АҚ, «QazaqGaz» ҰК АҚ, «ҚазМұнайГаз» ҰК АҚ, сондай-ақ Топтың жекелеген IT-компанияларында байқалды.

Есепті кезеңде деректер қауіпсіздігі саласындағы оқудан 9 194 жұмыскер өтті, олардың 40%-дан астамы Қазақстан Республикасы заңнамасының міндетті талаптарынан асатын бағдарламалар бойынша оқыды.
Білім беруіс-шараларының жиынтық көлемі 113 тренингаясында 17 077 сағатты құрады, бұл бір жұмыскерге орташа есеппен 0,54 сағатқа сәйкес келеді. Бұл тәсіл нормативтік талаптарды орындауға ғана емес, киберқауіпсіздіктің озық тәжірибелерін енгізу есебінен ақпараттық қауіпсіздік мәдениетінің деңгейін айтарлықтай арттыруға мүмкіндік берді.

2025 жылғы ақпараттық қауіпсіздік инциденттерінің саны



9 194 ЖҰМЫСКЕР

есепті кезеңде қауіпсіздік саласында оқудан өтті

17 077 САҒАТ

білім беру іс-шараларының жалпы көлемі

~0,54 сағат бір жұмыскерге

GRI 3-3