Ақпараттық қауіпсіздік және деректерді қорғау

GRI 418-1 Біз ақпараттың құпиялылығын, тұтастығын немесе қолжетімділігін бұзуы мүмкін ақпаратты және IT-активтерді рұқсатсыз қол жеткізуден және тәуекелдерден қорғау стратегияларын, әдістері мен процестерін қамтитын ақпараттық қауіпсіздікті басқарудың сенімді жүйесін дамытуға ұмтыламыз.

Ақпараттық қауіпсіздік саласындағы Қордың негізгі стратегиялық мақсаттары ақпараттық жүйелердің қолжетімділігін, тұтастығын, құпиялылығын және бас тартуға тұрақтылығын қамтамасыз ету болып табылады.

Ақпараттық қауіпсіздіктегі тәуекелдерді азайту үшін біздің қағидаттарымыз:

- кор жұмысының тұрақтылығы мен сенімділігіне теріс әсер етуге қабілетті ақпараттық технологиялардағы қатерлерді тез анықтау, талдау және дамыту болжамы;
- қолайсыз факторлардың әсерін бағалау;
- ақпараттық қауіпсіздік жөніндегі талаптардың басымдығы;
- ақпараттық қауіпсіздікті қамтамасыз етудің үздіксіздігі;
- шаралардың бақылану мүмкіндігі мен тиімділігі.

Қорда Ақпараттық қауіпсіздік жөніндегі комитет жұмыс істейді, ол ақпараттық қауіпсіздік деңгейін арттыруға бағытталған ұсынымдарды әзірлеуге жауап береді және осы мәселелерді тиімдірек шешу үшін мемлекеттік органдармен және басқа да мүдделі тараптармен тұрақты өзара іс-қимылды қолдайды.

GRI 3-3 GRI 418-1 Осы саладағы жүйелі тәсіл үшін біз «Ақпараттық қауіпсіздік саясатының негізгі ережелерін» әзірлеп, енгіздік, Олар әдістемелерді, нұсқаулықтар мен ережелерді қамтиды. Бұл құжаттар ақпараттық технологиялар саласындағы мамандардың да, Қордың барлық басқа жұмыскерлерінің де қауіпсіздік талаптарын сақтауын қамтамасыз етуге бағытталған.

Кейбір портфельдік компанияларда Ақпараттық қауіпсіздік саясаты енгізілген, олар олардың қызметінің ерекшелігін ескере отырып әзірленген және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы үздік халықаралық тәжірибелерге бағдарланған. Мысалы, ақпараттық қауіпсіздікті қамтамасыз ету және клиенттердің дербес деректерін қорғау үшін мыңдаған қазақстандықтарға байланыс қызметін көрсететін «Қазақтелеком» АҚ кешенді тәсілді ұстанады, олар компанияның инфрақұрылымына түскен сәттен бастап оларды мұрағаттауға немесе қайтарымсыз жоюға дейін олардың өмірлік циклінің барлық кезеңдерінде тәулік бойы бақылау жүргізеді. Бұдан басқа, компания ИҚБШ (Интернетке қол жеткізудің бірыңғай шлюзі) кибер қауіпсіздігінің мемлекеттік жүйесіне кіріктіру, Заттар Интернетінің қауіпсіздігі, Honeypot қақпандарын пайдалану (қаскүнемнің стратегиясын зерделеуге және нақты бар қауіпсіздік объектілеріне соққы берілуі мүмкін құралдардың тізбесін анықтауға мүмкіндік береді), Machine Learning технологияларын пайдалану сияқты қауіпсіздік элементтерін және басқа да бірқатар құралды пайдаланады.

GRI 3-3 Ақпараттық қауіпсіздік жүйесін жетілдіру шеңберінде біз деректерді қорғауға және Қор тобының ішіндегі іс-қимылдарды үйлестіруге бағытталған барлық негізгі қағидаттар мен ережелерді қамтитын Ақпараттық қауіпсіздіктің корпоративтік стандартын енгіздік. Корпоративтік стандарт Қор және оның портфельдік компаниялары үшін ақпараттық қауіпсіздік процестерін жүзеге асыру кезінде орындалуы міндетті болып табылады.

2024 жылы біз ақпараттық қауіпсіздікті нығайту бойынша жүйелі жұмысты жалғастырдық:

- ISO 27001 халықаралық стандартының ақпараттық қауіпсіздігін басқаруда үздік практиканы енгізуге дайындық басталды;
- IT инфрақұрылымының сенімділігі мен тиімділігі артты. Ақпараттық қауіпсіздіктің қазіргі заманғы талаптарына сәйкес ақпараттық ресурстардың тұрақты және қауіпсіз жұмысын қамтамасыз ететін техникалық және ұйымдастыру шаралары енгізілді;
- ақпараттың таралып кетуін болдырмау үшін қазіргі заманғы бағдарламалық өнімдер мен құралдарды, осалдықтарды сканерлеу және нақты уақыт режимінде қауіп-қатерлерді талдау құралдарын енгізуді қоса алғанда, сыртқы және ішкі қатерлерден қорғау жөніндегі шешімдер кешені іске асырылды;
- Киберорнықтылық деңгейін бақылау және арттыру шеңберінде екі портфельдік компанияда («Тау-Кен Самұрық» ҰТК» АҚ және «Samruk Kazyna Construction» АҚ) ақпараттық қауіпсіздік аудиттері жүргізілді. Тексеру қорытындысы бойынша анықталған тәуекелдерді жою бойынша ұсыныстар берілді;
- IT жүйелерімен және корпоративтік деректермен жұмыс істеу кезінде қауіпсіз тәртіп мәдениетін қалыптастыруға бағытталған жұмыскерлер үшін ақпараттық қауіпсіздік мәселелері бойынша оқыту іс-шаралары мен курстары өткізілді.

.

GRI 418-1 Есептік жылы ақпараттық қауіпсіздікке байланысты тіркелген инциденттердің жалпы саны 25 240 оқиғаны құрады, бұл 2023 жылмен салыстырғанда 57% -ға артық (2023 жылы – 16 094). Жағдайлардың 60% -ға жуығы зиянды бағдарламалық қамтамасыз етуді табуға және рұқсатсыз қол жеткізу/бұзу әрекеттеріне тиесілі. Есеп беру кезеңінде портфельдік компанияларда осы клиенттердің жылыстауы фактілері анықталған жоқ.