Ақпараттық қауіпсіздік

«Самұрық-Энерго» АҚ Ақпараттық қауіпсіздік (АҚ) саясатына сәйкес Компания ISO/IEC 27001 ақпараттық технология стандартына сәйкес қамтамасыз ету жөніндегі қызметті ұйымдастыруға ұмтылады Қауіпсіздік әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері. Осы мақсатта ішкі нормативтік құжаттар бекітіліп, келесі іс-шаралар жүргізілуде:

- АҚБЖ әзірлеу және өзектендіру;
- АҚ тәуекелдерін және ақпараттық активтер иелерін сәйкестендіру;
- АҚ тәуекелдерін бағалау және өңдеу;
- Бақылау іс-шараларын әзірлеуді/енгізуді үйлестіру;
- АҚ бойынша іс-шараларды орындау;
- АҚ тәуекелдерінің мониторингі, есептілік;
- АҚБЖ -ті жетілдіру.

Ақпараттық қауіпсіздікті қамтамасыз ету функциялары ақпараттандыру объектілерін құрумен, сүйемелдеумен және дамытумен айналысатын басқа құрылымдық бөлімшелерден оқшауланған құрылымдық бөлімше болып табылатын «Қауіпсіздік» департаментіне жүктелген. Бекітілген ұйымдық құрылымға сәйкес Департамент «Самұрық-Энерго» АҚ Басқарма төрағасына тікелей бағынады. АҚ бөлігінде бұл құрылымдық бөлімше келесі функцияларға жауап береді:

- нормативтік-өкімдік құжаттаманы және АҚ-ға қойылатын талаптарды әзірлеу;
- АҚ қамтамасыз ету мәселелері бойынша бизнес-бөлімшелер арасындағы өзара іс-қимылды қамтамасыз ету;
- АҚ бойынша талаптардың орындалуын бақылау;
- ақпараттық қауіпсіздікті қамтамасыз ету саласындағы ЕТҰ қызметінің мониторингі;
- қоғамның ақпараттық қауіпсіздігін қамтамасыз ету саласындағы мемлекеттік уәкілетті органдармен өзара іс-қимыл жасау;
- АҚ тәуекелдері бойынша іс-қимылдарды үйлестіруді жүзеге асыру;
- Ақпараттық қауіпсіздік жедел орталығымен өзара іс-қимыл.

АҚ қамтамасыз ету үдерісі шеңберінде компания мынадай негізгі бағыттарды ескереді:

- ақпараттық қауіпсіздікті басқару;
- ақпараттық қауіпсіздікті техникалық қамтамасыз ету;
- ақпараттық қауіпсіздік инциденттерін бақылау және оларға ден қою.

Ақ басқару процесі аясында Компания АҚ жұмысын реттейтін келесі құжаттарды әзірледі:

- «Самұрық-Энерго» АҚ Ақпараттық қауіпсіздік саясаты;
- «Самұрық-Энерго» АҚ-да ақпараттық жүйелердің ақпараттық қауіпсіздігін қамтамасыз ету қағидалары;
- «Самұрық-Энерго» АҚ-да құпия ақпараттың сақталуын қамтамасыз ету жөніндегі Нұсқаулық.

АҚ техникалық қамтамасыз ету функциясын «қауіпсіздік» департаменті және «Energy Solutions Center» ЖШС мамандары жүзеге асырады. Бұл функция компанияның ақпараттық активтерін қорғаудың бағдарламалық-техникалық тетіктерін қолдану арқылы АҚ-ны қамтамасыз ету процесін білдіреді. Қазіргі уақытта компанияның ақпараттық қауіпсіздігін қамтамасыз ету бойынша негізгі іс-шаралар:

- зиянды кодтан қорғауды қамтамасыз етудің бағдарламалық кешенін пайдалану арқылы компания мен филиалдардың корпоративтік желісін вирусқа қарсы қорғауды қамтамасыз ету;
- Компанияның корпоративтік желісінің және Интернет желісіне қолжетімділігі бар ресурстардың ақпараттық қауіпсіздік деңгейін арттыру үшін қолданылатын демилитаризацияланған аймақ (ДМА). ДМА Firewall пакеттік сүзгілерінің (брандмауэрлердің) бағдарламалық-аппараттық кешені базасында іске асырылды, бұдан басқа, бағдарламалық-аппараттық құралдармен тарату деңгейінде пакеттерді қосымша сүзу үшін басып кіруді болдырмау жүйесі іске асырылды. жіберілген және алынған электрондық хаттарды бақылау үшін қолданылатын бағдарламалық құралды басқару. Осы жүйенің көмегімен «Самұрық-Энерго» АҚ периметрі бойынша жөнелтушілердің спам-ларын бұғаттау және корпоративтік желіден тыс құпия ақпараттың ағып кетуін болдырмау үшін зиянды бағдарламалық қамтамасыз етудің болуына электрондық хаттарды талдау, бағдарламалық қамтамасыз етуді бақылау жүргізіледі.

АҚ инциденттеріне бақылау және ден қою функциясын «қауіпсіздік» департаментінің қызметкерлері және «Energy Solutions Center» ЖШС мамандары ақпараттық қауіпсіздік жедел орталығы (АҚЖО) және ақпараттық қауіпсіздік жөніндегі бағдарламалық-аппараттық кешен құралдарымен тіркейді:

- Қауіпсіздік оқиғалары журналдарын орталықтандырылған жинау, сақтау, талдау;
- Нақты уақыттағы оқиғаларды анықтау;
- Оқиғаларға басымдық беру;
- Инциденттерді түзету процесін бақылау және жауап беру уақытын сақтау (SLA);

- Нормативтік талаптардың сақталуы туралы есептер жасау.

АҚ инциденттерін бақылау және оларға ден қою жөніндегі нәтижелер мынадай есептерде жазылады:

- АҚЖО-мен шарт шеңберінде «Самұрық-Энерго» АҚ Ақпараттық қауіпсіздік инфрақұрылымының жай-күйін талдай отырып, ай сайынғы талдамалық есеп;
- «Самұрық-Энерго» АҚ Директорлар кеңесі үшін ақпараттық қауіпсіздік тәуекелдері бойынша тоқсан сайынғы есеп;
- Ақпараттық қауіпсіздікті (киберқауіпсіздікті) қамтамасыз ету, сондай-ақ «Самұрық-Энерго» АҚ Аудит жөніндегі Комитеті мен Директорлар кеңесі үшін ат-жүйелер мен инфрақұрылымды қорғау және қолдау бөлігінде «Самұрық-Энерго» АҚ Ішкі бақылауларының жеткіліктілігін талдау және бағалау жөніндегі жыл сайынғы есеп.

Жыл бойы Қоғам қызметкерлерінің хабардарлығын арттыру бойынша оқыту материалдарын (жадынамалар, скринсерверлер, бейнероликтер) әзірлеу туралы жұмыс жоспарын жыл сайын бекіту арқылы АҚБЖ туралы хабардарлықты арттыру жүргізіледі, АҚ бойынша инновациялар, талаптар және алдын алу шаралары туралы тарату жүзеге асырылады. Жыл сайынғы негізде қоғам қызметкерлері белгіленген тәртіппен ақпараттық қауіпсіздік нормаларын білуге онлайн тестілеу жүргізді.

2023 жылы барлық жаңадан қабылданған қызметкерлер үшін «Бейімдеу курсы» оқытылды, оған ақпараттық қауіпсіздік бойынша оқыту да кіреді.

GRI 418-1

Компанияда есепті кезеңде құпиялылықты бұзу, ағып кету, ұрлық және/немесе клиенттердің деректерін жоғалту туралы негізделген шағымдар тіркелген жоқ.

Ақпараттық қауіпсіздік жедел орталығы

«Самұрық-Энерго» АҚ келесі қызметтерді көрсететін «QazCloud» ЖШС-мен шарт шеңберінде ұсынылатын 24/7 режимінде ақпараттық қауіпсіздіктің барлық оқиғаларын мониторингілеу үшін ақпараттық қауіпсіздік жедел орталығына қосылды:

- ақпараттық қауіпсіздік оқиғаларын бақылау және басқару жүйелерімен және сыртқы периметрді қорғау жүйелерімен тіркелген АҚ оқиғаларының тәулік бойы мониторингі;
- Тапсырыс берушінің серверлік жабдықтарында және желілік құрылғыларында тіркелген АҚ оқиғаларының тәулік бойы мониторингі (бұдан әрі-мониторинг аймағы);
- мониторинг аймағында болған АҚ инциденттерін анықтау;
- тапсырыс берушіге анықталған инциденттер және оларға ден қою әдістері туралы ақпарат жолдау және оларды жою жөнінде ұсынымдар беру;
- инциденттерге ден қою процесінде сараптамалық қолдау көрсету;
- сыртқы Интернет желісінен Тапсырыс берушінің периметріне келетін оқыс оқиғаларға ден қою;
- АҚ инциденттеріне тергеу жүргізу;
- АҚ мониторингін (Red team және Blue team) қамтамасыз ету кезінде командалық өзара іс-қимылдан тұратын АҚЖО 3-деңгейлі қолдау желісі. Blue team 24/7 режимінде оқиғаларды бақылау және киберқауіптерге жауап беру арқылы инфрақұрылымды қорғауды қамтамасыз етеді. Red team инфрақұрылымның осалдығын кәсіби түрде анықтауға мүмкіндік береді;
- Веб-қосымшаларды қорғау және WEB трафигі;
- DDOS шабуылдарынан қорғау;
- АҚ апта сайынғы дайджесті;
- Сондай-ақ, ену және осалдықтарды анықтау үшін сыртқы тестілеуді қамтитын аудит (penetration test) жүргізу.

Компанияның киберқауіпсіздік саласындағы бастамалары «Самұрық-Энерго» АҚ-ның 2023-2025 жылдарға арналған ақпараттық технологиялар және цифрландыру Стратегиясында бекітілген.