Ивченко Елена Дмитриевна

GR, Даму және IT бойынша басқарушы директор

Цифрландыру біз үшін – уақыт талаптары мен біздің серіктестер мен қызметкерлердің күтуіне негізделген стратегиялық қажеттілік.

Біз негізгі процестерді – төлем жүргізу, архивті сақтау, комплаенс қызметін – цифрлық форматқа көшірдік, осылайша бизнес-процестердің ашықтығын, жылдамдығын және басқарылуын арттырдық. Бұл тек бастамасы ғана. Алда өндірістік деректерді автоматтандыру, интеллектуалды мониторинг жүйелерін енгізу, болжам жасау және шешім қабылдау үшін жасанды интеллектті пайдалану тұр. Цифрлық трансформация – Компанияның дамуының негізгі бағыттарының бірі болып табылады және біз бұл жолды жүйелі әрі ұдайы жалғастыруға ниеттіміз.

Ақпараттық қауіпсіздік

GRI 3-3

«Самұрық-Энерго» АҚ Ақпараттық қауіпсіздік саясатына сәйкес Компания ҚР СТ ISO 27001 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Ақпараттық қауіпсіздікті басқару жүйелері» халықаралық стандартына сәйкес келетін ақпаратты қорғау жүйесін құруға бағытталған. Осы мақсатты іске асыру үшін ішкі нормативтік құжаттар әзірленіп, бекітілді, сондай-ақ мынадай негізгі іс-шаралар енгізілуде:

- Ақпараттық қауіпсіздікті басқару жүйесін (АҚБЖ) әзірлеу және өзектендіру;
- Ақпараттық қауіпсіздік тәуекелдерін анықтау және ақпараттық активтердің иелерін айқындау;
- Ақпараттық қауіпсіздік тәуекелдерін бағалау және өңдеу;
- Бақылау іс-шараларын әзірлеу мен енгізуді үйлестіру;
- Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі іс-шараларды орындау;
- Ақпараттық қауіпсіздік тәуекелдерінің мониторингі және есептілікті дайындау;
- Ақпараттық қауіпсіздікті басқару жүйесін үздіксіз жетілдіру.

Компаниядағы ақпараттық қауіпсіздікті қамтамасыз ету жауапкершілігі дербес құрылымдық бөлімше болып табылатын және «Самұрық-Энерго» АҚ Басқарма төрағасына тікелей бағынатын Қауіпсіздік департаментіне жүктелген. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі өз қызметі шеңберінде бөлімше мынадай негізгі функцияларды орындайды:

- Ақпараттық қауіпсіздік бойынша нормативтік-өкімдік құжаттаманы және талаптарды әзірлеу;
- Ақпараттық қауіпсіздік мәселелері бойынша бизнес-бөлімшелер арасындағы өзара әрекеттесуді қамтамасыз ету;
- Ақпараттық қауіпсіздік талаптарының сақталуын бақылау;
- Ақпараттық қауіпсіздік саласындағы ЕТҰ қызметінің мониторингі;
- Қоғамның ақпараттық қауіпсіздігі мәселелері бойынша мемлекеттік органдармен өзара әрекеттесуі;
- Ақпараттық қауіпсіздік тәуекелдерін басқару жөніндегі іс-әрекеттерді үйлестіру;
- Ақпараттық қауіпсіздіктің жедел орталығымен өзара әрекеттесуі.

АҚ-ны қамтамасыз ету процесінде компанияда үш негізгі бағыт ескеріледі:

- Ақпараттық қауіпсіздікті басқару;
- Ақпараттық қауіпсіздікті техникалық қамтамасыз ету;
- Ақпараттық қауіпсіздіктің оқыс оқиғаларын бақылау және оларға ден қою.

Ақпараттық қауіпсіздікті басқару

Ақпараттық қауіпсіздікті басқару процесінің шеңберінде Компанияда осы саладағы жұмысты реттейтін бірқатар құжаттар әзірленді:

- «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.

Ақпараттық қауіпсіздікті техникалық қамтамасыз ету

Ақпараттық қауіпсіздікті техникалық қамтамасыз ету функциясын Қауіпсіздік департаменті «Energy Solutions Center» ЖШС мамандарымен бірлесіп жүзеге асырады. Техникалық қамтамасыз ету қазіргі заманғы бағдарламалық-техникалық құралдарды пайдалана отырып, компанияның ақпараттық активтерін қорғауға бағытталған іс-шаралар кешенін білдіреді.

Осы функция шеңберінде орындалатын негізгі іс-шаралар:

- Зиянды кодтан қорғау үшін мамандандырылған бағдарламалық жасақтаманы қолдана отырып корпоративтік желіні және филиалдарды вирусқа қарсы қорғауды қамтамасыз ету;
- Интернетке қол жеткізе отырып, корпоративтік желі мен ресурстардың ақпараттық қауіпсіздік деңгейін арттыру үшін демилитаризацияланған аймақты (ДМА) құру. ДМА Firewall пакеттік сүзгілерінің (брандмауэрлердің) бағдарламалық-аппараттық кешені негізінде іске асырылды, бұл пакеттерді тарату деңгейінде қосымша сүзуді қамтамасыз етеді;
- Жіберілетін және алынатын электрондық хаттарды бақылау үшін бағдарламалық жасақтаманы бақылау. Жүйе «Самұрық-Энерго» АҚ периметрі бойынша спам-жіберушілерді бұғаттауға, зиянды бағдарламалардың болуына электрондық хаттарды талдауға және корпоративтік желіден тыс құпия ақпараттың таралып кетуіне жол бермеуге мүмкіндік береді.

Ақпараттық қауіпсіздік оқыс оқиғаларын бақылау және оларға ден қою

Ақпараттық қауіпсіздік оқыс оқиғаларын бақылау және оларға ден қою функциясын Қауіпсіздік департаментінің қызметкерлері «Energy Solutions Center» ЖШС мамандарымен бірлесіп орындайды. Барлық оқыс оқиғалар АҚ-ны қамтамасыз ету үшін бағдарламалық-аппараттық кешенді пайдалана отырып, ақпараттық қауіпсіздіктің жедел орталығында (АҚЖО) тіркеледі және өңделеді.

Негізгі оқиғаларға мыналар жатады:

- Қауіпсіздік оқиғаларының журналдарын орталықтандырылған жинау, сақтау және талдау;
- Нақты уақытта оқыс оқиғаларды анықтау;
- Оқыс оқиғалардың басымдықтарын айқындау;
- Оқыс оқиғаларды түзету процесін бақылау және әрекет ету уақытын сақтау;
- Нормативтік талаптардың сақталуы туралы есептер жасау.

Оқыс оқиғаларды бақылау және оларға ден қою нәтижелері келесі есептерде құжатталады:

- Ақпараттық қауіпсіздік жөніндегі операциялық орталықпен шарт жасасу шеңберінде «Самұрық-Энерго» АҚ ақпараттық қауіпсіздік инфрақұрылымының жай-күйін талдауды қамтитын ай сайынғы талдамалық есеп;
- «Самұрық-Энерго» АҚ Директорлар кеңесі үшін ақпараттық қауіпсіздік тәуекелдері бойынша тоқсан сайынғы есеп;
- Ақпараттық қауіпсіздікті (киберқауіпсіздікті) қамтамасыз ету жөніндегі жыл сайынғы есеп, сондай-ақ Аудит жөніндегі комитет пен Директорлар кеңесі үшін «Самұрық-Энерго» АҚ Ішкі бақылауларының жеткіліктілігін талдау және бағалау.

Есепті кезең ішінде ақпараттық қауіпсіздікті басқару жүйесі туралы хабардарлық деңгейін арттыру бойынша жұмыстар жүргізілді. Жыл сайын Қоғамның барлық қызметкерлері үшін жадынамалар, скринсерверлер және бейнероликтер сияқты оқу материалдары әзірленетін жұмыс жоспары бекітіледі. Сондай-ақ ақпараттық қауіпсіздік бойынша жаңа енгізілімдер, талаптар және алдын алу шаралары туралы тарату жүзеге асырылады. Жыл сайын Қоғамның барлық қызметкерлері ақпараттық қауіпсіздік нормаларын білу үшін онлайн-тестілеуден өтеді, бұл олардың осы саладағы құзыреттілігін растайды.

Жұмысқа қабылдау кезінде барлық жаңа қызметкерлер ақпараттық қауіпсіздік бойынша оқытуды қамтитын «Бейімдеу курсынан» өтеді. 2024 жылы бұл оқыту барлық жаңадан қабылданған қызметкерлер үшін жүргізілді, бұл олардың компанияда жұмыс істеген кезінен бастап ақпараттық қауіпсіздік стандарттары туралы жоғары хабардарлық пен сәйкестікті қамтамасыз етуге мүмкіндік береді.

GRI 418-1

Есепті кезеңде Компанияда құпиялылықтың бұзылуына, ағып кетуіне, ұрлануына немесе клиенттер деректерінің жоғалуына қатысты бірде-бір негізделген шағым тіркелген жоқ

Ақпараттық қауіпсіздіктің жедел орталығы

«Самұрық-Энерго» АҚ-ның ақпараттық қауіпсіздік жедел орталығы 24/7 режимінде ақпараттық қауіпсіздіктің барлық оқиғаларының мониторингін жүзеге асыратын Ақпараттық қауіпсіздік жедел орталығына (бұдан әрі – АҚЖО) қосылған. АҚЖО мынадай қызметтерді көрсететін «QazCloud» ЖШС-мен келісімшарт шеңберінде ұсынылады:

- Ақпараттық қауіпсіздік оқиғаларын бақылау және басқару жүйелерімен, сондай-ақ сыртқы периметрді қорғау жүйелерімен тіркелген Ақпараттық қауіпсіздік оқиғаларының тәулік бойы мониторингі;
- Серверлік жабдықта және желілік құрылғыларда болып жатқан ақпараттық қауіпсіздік оқиғаларының тәулік бойы мониторингі (бұдан әрі – Мониторинг аймағы);
- Мониторинг аймағында болатын ақпараттық қауіпсіздік оқиғаларын анықтау;
- Анықталған оқиғаларды, сондай-ақ оларға ден қою әдістерін және оларды жою жөніндегі ұсынымдарды тіркеу;
- Оқыс оқиғаларға ден қою процесінде сараптамалық қолдау көрсету;
- Ақпараттық қауіпсіздіктің оқыс оқиғаларына терген-тексеру жүргізу;
- Red team және Blue team кіретін АҚ мониторингін қамтамасыз ету бойынша топтық жұмыстан тұратын үш деңгейлі АҚЖО-ны қолдау желісі. Blue team тәулік бойы оқиғаларды бақылау және киберқауіптерге жауап беру арқылы инфрақұрылымды қорғаумен айналысады. Red team, өз кезегінде, инфрақұрылымның осалдығын кәсіби түрде анықтайды;
- Веб-қосымшалары мен WEB трафигін қорғау;
- DDOS шабуылдарынан қорғау;
- Ақпараттық қауіпсіздік бойынша апталық дайджест;
- Сыртқы ену тестілеуін және осалдықтарды анықтауды қамтитын Аудит (penetration test).