Ауылдық жерлерде тіркелген сымсыз қолжетімділікті (FWA) дамыту

«Ауыл Телеком» ЖШС еншілес компаниясы ауылдық жерлерде тіркелген сымсыз қолжетімділікті (FWA) дамыту бойынша пилоттық жобаларды іске асыруда. Бұл – ТОБЖ немесе GPON желілерін салу экономикалық тұрғыдан тиімсіз болатын жерлерде жоғары жылдамдықты интернетпен қамтамасыз етуге мүмкіндік береді. Аталған бастама цифрлық теңсіздікті азайтып, шалғай өңірлердің тұрғындарын заманауи байланыспен қамтуға жол ашады.

Пилоттық жобалар аясында Open RAN және FWA 5G негізіндегі шешімдер сыналды. Сарыбай ауылында қосылу жылдамдығы орта есеппен 85 есеге артып, 5 Мбит/с-тан 427 Мбит/с-қа жетті. Бұл онлайн-білім беру, телемедицина және қашықтан жұмыс сапасын едәуір жақсартуға мүмкіндік берді. Осылайша, FWA ескі технологияларды (WiFi, ADSL, CDMA EVDO) жаңғыртуды қамтамасыз етіп қана қоймай, қала мен ауыл арасындағы цифрлық алшақтықты жоюға бағытталған негізгі құралға айналуда.

«Ауыл Телеком» компаниясы FWA желісін белсенді кеңейтуді жалғастыруда, ал 5G технологиясы компания үшін стратегиялық бағыт болып табылады. Дегенмен, бір мезгілде 4G желісі де құрылып жатыр. Ақтөбе облысының Қаратала ауылындағы жоба сәтті іске асырылған мысал ретінде келтірілуі мүмкін – мұнда 120 тұрғын үйдің 79-ы желіге қосылған. Қосылымның орташа жылдамдығы 46 Мбит/с құрайды, ал бір тұрғын үйге шаққандағы үш аптадағы интернет трафигінің орташа көлемі 191 ГБ-ға жетті. 10 абоненттің трафик көлемі осы кезеңде 450 ГБ-дан асып кетті.

Әртүрлі желілік функциялар мен техникалық шешімдерді сынау

- Open RAN 5G Fronthaul негізіндегі бағдарламалық-аппараттық кешен арқылы тіркелген сымсыз қолжетімділік (Fixed Wireless Access) технологиясы бойынша интернетке қолжетімділікті қамтамасыз ету үшін техникалық мүмкіндік пен дайындық сынақтан өткізілді. Open RAN 5G Fronthaul БАК-тың жұмысқа жарамдылығы кейбір шектеулермен расталды.
- TelcoCloud бұлттық ортасындағы «Қазақтелеком» АҚ желісінде желілік трафик статистикасын мониторингілеу және талдау мүмкіндіктерін анықтау мақсатында invGUARD AS-SW бағдарламалық кешені сынақтан өткізілді.
- Қонаев қаласында TelcoCloud бұлттық ортасында VOLTHA GPON технологиясы тестілеуден өткізілді. Бұл шешімнің негізгі идеясы – дезагрегация және өндірушіге тәуелділіктен арылу. Классикалық GPON жүйесінде OLT жабдығы (стационарлық), бағдарламалық жасақтама, лицензиялар және ONT (клиенттік) бір ғана өндірушіден жеткізіледі және бір-бірімен «байланыстырылған», бұл басқа өндірушілердің ONT құрылғыларын басқа вендордың OLT жабдығына қосуға немесе басқа өндірушінің бағдарламалық жасақтам
- Өнім әлі толығымен дайын емес, бірақ идеяның өзі және іс-әрекеттер нәтиже береді. Қонаев қаласында VOLTHA платформасы негізіндегі КЖҚ пилоттық жобасы іске қосылды.
- Қазақстан және Орталық Азия желі операторларына кэш-серверлеріне қатынау қызметі тексерілді.
- Сондай-ақ, PicoCell технологиясы арқылы интернетке мобильді қатынауды қамтамасыз ететін indoor-шешім сынақтан өтіп жатыр. Бұл шешім мобильді байланыс/КЖҚ сапасы төмен жерлерде (жертөле үй-жайларындағы дүкендер, кафелер) қолданылады.

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӘНЕ ДЕРЕКТЕРДІ ҚОРҒАУ

Компания ақпараттық қауіпсіздікті қамтамасыз етудің және өз клиенттерінің деректерін қорғаудың маңыздылығын түсінеді. «Қазақтелеком» АҚ-да ақпараттық қауіпсіздік пен деректерді қорғауды басқарудың сенімді жүйесін дамыту жалғасуда.

БАСҚАРУ ТӘСІЛІ

GRI 3-3, 418-1

Ақпараттық қауіпсіздік қызметі – Компаниядағы ақпараттық қауіпсіздік мәселелерін жоғары деңгейде қадағалайтын Ақпараттық қауіпсіздік жөніндегі басқарушы директорға тікелей бағынады.

Ақпараттық қауіпсіздік саласындағы мәселелерді реттейтін негізгі ішкі құжаттар:

- Ақпараттық қауіпсіздік саясаты.
- «Қазақтелеком» АҚ-да жеке деректерді қорғау саясаты.
- Ақпараттық қауіпсіздік тұжырымдамасы.

Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі қағидаттары:

> Компанияның ақпараттық қауіпсіздік саласындағы мәселелерін реттейтін құжаттарымен Компанияның ресми сайтындағы «Тұрақты даму» бөліміндегі «Ақпараттық қауіпсіздік және деректерді қорғау» қосымша бөлімінде танысуға болады.

- заңнамалық нормаларды орындау;
- Қоғамның жоғары басшылығының АҚ-ны қамтамасыз ету процесіне қатысуы;
- бизнеске бағдарлану;
- процестік тәсіл;
- ақпаратты қорғау тәсілдерін, әдістері мен құралдарын кешенді пайдалану;
- үздік тәжірибелерді ұстану;
- ақылға қонымды жеткіліктілік;
- хабардарлық және жеке жауапкершілік.

Ақпараттық қауіпсіздікті қамтамасыз ету үшін «Қазақтелеком» АҚ жүйелі тәсілді қолданады. Маңызды аспектілердің бірі – деректерді Компанияның инфрақұрылымына енген сәттен бастап мұрағаттауға немесе қайтарымсыз жоюға дейінгі өмірлік циклінің барлық кезеңдеріндегі оларды тәулік бойы бақылау.

Қазіргі уақытта Компанияда ақпараттық қауіпсіздікті қамтамасыз ету әдістерінің үздік әлемдік тәжірибелері қолданылады. Біздің ішкі жүйелеріміз ақпараттық ресурстарға қауіпсіз қашықтан қол жеткізу, интернетті қауіпсіз пайдалану, артықшылықты пайдаланушыларды (PAM) бақылау, осалдық сканерлері және т.б. сияқты шешімдермен қорғалған. Компания сыртқы қауіптерге қарсы тұруға ұмтылады және ресурстармен жұмыс істеудің жаңа шешімдері мен әдістерін, соның ішінде Компанияда қажетті инфрақұрылымды құруды, білікті мамандарды оқытуды, ақпараттық қауіпсіздіктің жедел орталығын қалыптастыруды және ZeroTrust тұжырымдамасын енгізеді.

Сонымен бірге, Компания ИҚБШ мемлекеттік киберқауіпсіздік жүйесіне кіріктіру, интернет заттарының қауіпсіздігі, Machine Learning, Honeypot тұзақтарын пайдалану және т.б. сияқты маңызды қауіпсіздік элементтерін пайдаланады. Бұдан басқа, Компания қызметкерлерін оқыту және АҚ-хабардарлығын арттыру тұрақты негізде жүргізіледі.

Дербес деректерді қорғау

GRI 418-1

Компанияда «Дербес деректерді қорғау саясаты» әзірленді және енгізілді, онда клиенттердің, жеткізушілердің, іскер серіктестердің, қызметкерлердің және басқа да тұлғалардың дербес деректерін өңдеудің негізгі қағидаттары айқындалды, сондай-ақ дербес деректерді жинау, сақтау және өңдеу жөніндегі негізгі іс-әрекеттер мен оларды қорғау жөніндегі шаралар айқындалды.

Саясат дербес деректерді қорғау саласындағы негізгі құжат болып табылады және Қоғам өз қызметінде басшылыққа алатын дербес деректерді қорғау саласындағы мақсаттарды, міндеттерді және қағидаттарды белгілейді. Сонымен қатар, дербес деректерді қорғаудың тиісті құжаттарын әзірлеу кезінде басшылық ретінде қызмет етеді.

Дербес деректерді қорғауды қамтамасыз етудің негізгі қағидаттары:

- адамның және азаматтың конституциялық құқықтары мен бостандықтарын қорғау;
- дербес деректерді қорғауды қамтамасыз етудің заңдылығы;
- қолжетімділігі шектеулі дербес деректердің құпиялылығы;
- Қоғам басшылығының дербес деректерді қорғауды қамтамасыз ету процесіне қатысуы;
- бизнеске бағдарлану;
- процестік тәсіл;
- қорғау тәсілдерін, әдістері мен құралдарын кешенді пайдалану;
- үздік тәжірибелерді ұстану;
- ақылға қонымды жеткіліктілік;
- ақпараттандыру және дербес жауапкершілік.

Есепті кезеңдегі негізгі нәтижелер

2024 жылы ақпараттық қауіпсіздік саласында Компанияда корпоративтік ақпараттық жүйелерді, дербес деректерді, қызметтік ақпаратты және деректерді беру желілерін қорғауды қамтамасыз ету мақсатында кешенді іс-шаралар жүргізілді.

Ақпараттық қауіпсіздікті басқару жүйесін өзектілігін сақтау шеңберінде Компанияда 16 нормативтік-құқықтық құжат бекітілді.

«Қазақтелеком» АҚ қызметкерлерінің ақпараттық қауіпсіздікті қамтамасыз ету саласындағы хабардарлық деңгейін арттыру шеңберінде 7 ақпараттық материал таратылып, Корпоративтік университеттің оқу порталы базасында ақпараттық қауіпсіздік ережелері мен талаптары туралы 2 цифрлық марафон іске қосылды, сондай-ақ кибергигиена саласындағы қызметкерлердің хабардарлығын бағалау және күдікті хаттарды алған кездегі пайдаланушылар әрекеттерін пысықтау мақсатында фишингтік хаттарды тарату түрінде 4 кибержаттығу өткізілді.

2024 жылы Компанияда Ақпараттық-коммуникациялық инфрақұрылымның аса маңызды объектілеріне (АҚИМО) жатқызылған жабдық орнатылған объектілерге/серверлік бөлмелерге, сондай-ақ осы жабдықты сүйемелдейтін/әкімшілік ететін құрылымдық бөлімшелерге кешенді тексеру жүргізілді. Анықталған сәйкессіздіктер бойынша филиалдардың құрылымдық бөлімшелерінің басшыларына ұсынымдар берілді.

Ақпараттық қауіпсіздік бойынша жедел жұмыс аясында 2024 жылы IT дивизионы құрылымдық бөлімшелердің жұмысын қайта ұйымдастырып, корпоративтік Ақпараттық қауіпсіздіктің жедел орталығын (АҚЖО) іске қосу және 24/7 жұмыс режиміне көшу жұмыстарын жүргізді. Негізгі міндеттері:

- Компанияның корпоративтік периметрін қорғау;
- Ақпараттық қауіпсіздік (АҚ) оқиғаларын мониторингілеу;
- АҚ инциденттеріне әрекет ету;
- АҚ инциденттерін тергеп-тексеру;
- Компанияның ақпараттық жүйелеріндегі осал тұстарды анықтау;
- Ақпараттық қауіпсіздік инциденттерін жою бойынша ұсынымдар беру;
- Ақпаратты қорғау құралдарын (АҚҚ) бақылау.

2024 жылы Компанияның ZeroTrust моделіне көшуінің екінші кезеңі жүзеге асырылды, ақпаратты қорғаудың бірқатар бағдарламалық-аппараттық құралдары (АҚҚ) енгізілді. Бұл Компанияның корпоративтік инфрақұрылымының қолданыстағы қорғанысын күшейтуге мүмкіндік берді. Корпоративтік АҚЖО жұмысының нәтижелері:

- 2024 жылы Компания клиенттерінің ресурстарына бағытталған шамамен 3 300 DDOS шабуылының жолы кесілді (ең жоғары жылдамдығы 74 Гбит/сек-тан астам), жалпы трафик 1 100 Тбит-тан асты;
- 710 миллионнан астам зиянды трафик пакеттері бұғатталды;
- Бағдарламалық жасақтамалар (БЖ) осалдықтарын сканерлеу құралдары арқылы Компанияда пайдаланылатын БЖ-да шамамен 118 мың осалдық анықталды, олардың 64%-дан астамы жауапты әкімшілер тарапынан жойылды;
- Ақпараттық қауіпсіздік құралдарының көмегімен 40 мыңнан астам желілік шабуылдың жолы кесілді, 45 мың вирус анықталды, 20 мыңнан астам құпиясөзді іріктеу әрекеті бұғатталды.
- PAM (Privileged Access Management – артықшылықты пайдаланушыларды басқару жүйесі) арқылы 120-дан астам IP-мекенжайы бар Корпоративтік ақпараттық жүйелердің терминалдық серверлерінде 270-тен астам артықшылықты пайдаланушы (ақпараттық жүйелер әкімшілері, сыртқы пайдаланушылар мен мердігерлер) бақыланады.
- DLP (Data Leak Prevention – деректердің сыртқа шығып кетуінің алдын алу) жүйесі арқылы ақпараттық қауіпсіздік талаптарын бұза отырып сақталған 800-ден астам құпия файл анықталды.
- Компанияның ақпараттық жүйелері мен ресурстарына толық еліктейтін шамамен 60 тұзақ (Honeypot) орналастырылды, бұл Компанияның корпоративтік желісі ішінде 2 000-нан астам зиянды сұранысты анықтауға мүмкіндік берді.

Есепті кезеңде клиенттің дербес деректерін өңдеудің ықтимал бұзылуына қатысты жедел желі бойынша бір өтініш тіркелді. Клиент деректерінің таралу фактісі расталмады.Есепті кезеңде Компанияда деректерінің таралу фактілері анықталған жоқ.

Ақпараттық қауіпсіздік мәселелері бойынша қызметкерлерді ақпараттандыру және оқыту

GRI 418-1

Компанияда ақпараттық қауіпсіздіктің негізгі қағидаттары – деректердің құпиялылығы, тұтастығы және қолжетімділігін қамтамасыз ету мақсатында қызметкерлер арасында оқыту іс-шаралары жүйелі түрде өткізіледі.

Ақпараттық қауіпсіздік әкімшілік деңгейде де – әрбір қызметкер Компанияның ақпараттық қауіпсіздік саласындағы регламенттерінің, ережелерінің, саясаттарының талаптарымен танысуға және орындауға міндетті, сондай-ақ техникалық және физикалық деңгейде де қамтамасыз етіледі – Компанияда әртүрлі аппараттық-бағдарламалық кешендер, ақпаратты криптографиялық қорғау құралдары және т.б. пайдаланылады.

Сонымен қатар, АҚ дивизионының мамандары ақпараттық қауіпсіздік, киберқауіпсіздік, АҚ тәуекелдері мен қауіптері бойынша біліктілікті арттыру курстарынан тұрақты түрде өтеді. Деректерді дұрыс пайдаланбау қаупі жоғары клиенттермен жұмыс жасау және персоналмен жұмыс жасау бөлімшелерінің қызметкерлері үшін цифрлық гигиена бойынша жалпы оқыту/тестілеу жүргізіледі.