.KZ және .ҚАЗ домендеріне арналған DNSSEC саясаты

1. КІРІСПЕ

1.1 Құжатта келесі негізгі ұғымдар мен қысқартулар қолданылады:

1) DNS – бұл домендік атаулар жүйесіне қызмет көрсетуге арналған арнайы бағдарламалық қамтылым, сонымен қатар бағдарламалық қамтылым орындалатын жабдық;

2) DNSSEC – дереккөздің аутентификациясын қолдауды қосатын және домендік атаулар жүйесі үшін деректердің тұтастығын тексеретін DNS кеңейтімі;

3) DS-жазба - жазба бір деңгейден төмен орналасқан аймақ (өкілетті аймақ) мекенжай ақпаратын куәландыру (қол қою) үшін пайдалануы тиіс кілтке нұсқайды.

4) DNSKEY-жазба-кілттің жалпыға ортақ бөлігін және оның идентификаторларын (ID, түрі және қолданылатын хэш функциясы) қамтиды;

5) KSK – DNSKEY ресурстық жазбасына қол қою кілті;

6) ZSK – ресурстық жазбаларға қол қою кілті;

7) HSM – аппараттық қорғаныс модулі;

8) Қосалқы домен - екінші, үшінші және одан да көп деңгейлердің домені.

2. ЖАЛПЫ МӘЛІМЕТТЕР

2.1 Бұл құжат .KZ және .ҚАЗ жоғары деңгейлі домендерінде DNSSEC жұмыс істеуінің негізгі рәсімдерін сипаттайды

2.2 Жоғарғы деңгейдегі домендерді Тіркеу бөлімі DNSSEC жұмыс істеу саясатын өзі анықтайды:

1) KSK басқарады;
2) аккредиттелген тіркеушіден алынған DNSSEC деректерін тексереді және өңдейді;
3) жоғарғы деңгейдегі домен файлында ресурстық жазбаларды қалыптастырады және қол қояды;
4) ZSK басқарады және жоғары деңгейлі домен файлын рұқсат етілген DNS серверлеріне таратады.

2.3 Тіркеуші домен тіркелушісінің атынан тізілімде тіркеу әрекеттерін жүзеге асырады. Тіркеуші домендік атауының тіркелушісіне тиесілі KSK кілтін тексеруге жауапты.

2.4 Домендік атаулардың тіркелушілері аккредиттелген тіркеушілердің көмегімен қажетті өзгерістер енгізеді және өздерінің домендік аймағына қол қоюдың дұрыстығына, сондай-ақ олардың қажеттіліктеріне сәйкес DS-жазбалар түрінде тізілімде орналастырылған ашық кілттердің өзектілігіне жауап береді.

2.5 Мүдделі тараптар – DNSSEC жұмысына сүйенетін Интернет желісінің мүшелері, мысалы, DNS серверлерін тексеру, олардың жабдықтарында тиісті сенімді ашық кілттерді орнатуға және жаңартуға жауапты.

2.6 DNSSEC-ті қосалқы домендерде пайдалану осы құжаттың ауқымынан тыс және осы домендерді тіркеушілер сипаттайды.

3. ПАЙДАЛАНУ ТАЛАПТАРЫ

3.1 Тіркеу бөлімі DNSSEC сенім тізбегін DNS түбірлік аймағында тікелей DS жазбасы түрінде ашық KSK жариялау арқылы құрайды.

3.2 DNSSEC-ті қосалқы доменде белсендіру үшін жоғарғы деңгейдегі домендер тізілімінде кем дегенде бір DS жазбасын орналастыру қажет. Тіркеу бөлімі кілт тегінің DS жазбасы қалыптасқан алгоритм тізілімінің қолдауын тексеру арқылы деректердің дұрыстығын тексереді. Егер DS жазбасын тексеру сәтті болса, онда берілген доменге арналған DS жазбасы DNS-те жарияланады. Жарияланған DS жазбасы қосалқы домен үшін сенім тізбегін орнатады.

3.3 Қосалқы доменді тіркелушінің сенімді сәйкестендіруі және аутентификациясы тіркеушінің міндеттеріне сәйкес келеді.

3.4 Тіркеу бөлімі EPP интерфейсін қолдана отырып, тіркеушілерден DS-жазбаларын қабылдайды. DS және DNSKEY жазбалары дұрыс болуы және RFC 4310-да сипатталған форматта жіберілуі керек. Тіркеу бөлімінің тізілімі RFC 4034 және RFC 5933 сәйкес құрылған DS жазбаларын орналастыруды қолдайды.

3.5 Тіркеу бөлімі қосалқы домен тіркелушісінің жеке кілті бар екенін сенімді анықтау мақсатында қосымша тексерулер жүргізбейді. Тиісті тексерулерді орындау тіркеушілерге жүктеледі.

3.6 Тіркеу бөлімі тіркеушіден EPP-интерфейсі арқылы тиісті сұрауды алған кезде DS-жазбасын тізілімнен жояды. Қосалқы домен үшін барлық DS-жазбаларын жою сол домен үшін DNSSEC өшіреді. Тек қосалқы доменді тіркелуші немесе тіркелушінің мүдделерін білдіруге ресми уәкілетті тарап қана тіркеушінің көмегімен осы домен үшін DS-жазбасын жою туралы сұрау жібере алады.

4. БАСҚАРУ ҚҰРАЛДАРЫ ЖӘНЕ ПАЙДАЛАНУ БАҚЫЛАУЫ

4.1 Тіркеу бөлімінің Қазақстан аумағында деректерді өңдеу орталығы (ДӨО) бар. ДӨО рұқсатсыз кіруден қорғалған сервер тіректерін қамтиды. Үздіксіз қуат көздерімен және ауаны баптау жүйелерімен жабдықталған. Орталықтандырылған өрт сөндіру жүйесі қосылған.

4.2 Кеңседе рәсімдерді өткізуге арналған бөлме дайындалды. Тіркеу бөлімінің объектілеріне шектеулі қолжетімділік ұйымдастырылған, ол тек уәкілетті персоналға ғана беріледі.

4.3 Маңызды ақпарат тасығыштар мен резервтік көшірмелер сейфтерде орналастырылады, оларға қол жеткізу тек уәкілетті персоналға ғана беріледі. Сыни құжаттар ұсақтау әдісімен жойылады. Электрондық ақпарат тасығыштар кәдеге жаратпас бұрын осы тасығыштарға бұрын жазылған ақпаратты қалпына келтіру мүмкіндігін болдырмау үшін арнайы форматтаудан өтеді.

4.4 Жабық KSK және ZSK кілттерімен жұмыс істеу үшін екі сенімді рөл құрылды: крипто-офицер және крипто-оператор, олардың әрқайсысы кем дегенде екі рұқсат етілген адамнан тұрады. Рұқсат етілген адамдардың әрқайсысының жеке идентификаторы және оған паролі

болады. Жабық KSK және ZSK кілттерімен жұмыс істеуге тартылған қызметкер бір уақытта крипто-офицер мен крипто-оператор рөлдерін біріктіре алмайды.

4.5 Негізгі рәсімдердің орындалу барысын бақылау үшін рөл құрылды: Бақылаушы, ол кем дегенде екі рұқсат етілген адамнан тұрады. Бақылаушылар KSK және ZSK кілттерінің құпия бөліктерімен маңызды операцияларды орындау кезінде процестің ашықтығын және рәсімдердің мұқият орындалуын қамтамасыз етеді.

4.6 Жоғарыда аталған персонал Тіркеу бөлімінің қызметкерлері болып табылады. Рәсімдерде қатысатын қызметкерлердің DNSSEC қолдану тәжірибесі болуы керек. Жаңа қызметкерлер жоғарыда аталған рөлдерге кіріспес бұрын DNSSEC іске асырылуын сипаттайтын ішкі құжаттаманы зерттеуі керек. Олар сондай-ақ өз міндеттерін орындауды бастамас бұрын бақылаушы ретінде негізгі рәсімдерге қатысуы керек.

4.7 DNSSEC маңызды ақпаратпен арнайы бөлінген жұмыс аймағына кірудің әрбір фактісі автоматтандырылған есепке алу жүйесінде сақталады. Қол жеткізуді есепке алудың автоматтандырылған жүйесі үнемі қаралып, талданады. Талдау жиілігі тіркеу бөлімінің ақпараттық қауіпсіздік саясатымен анықталады.

4.8 Егер қандай да бір оқиға қауіпсіздіктің бұзылуына әкеп соқтырса немесе әкелуі мүмкін болса, онда болған оқиғаның себептерін анықтау және оларды жою мақсатында ішкі тергеу жүргізіледі. Егер бұл оқиға DNSSEC-тің маңызды ақпаратына нұқсан келтірсе, онда кілттер апаттық түрде ауыстырылады. Кілттерді апаттық ауыстыру рәсімін крипто-оператор бастайды. Кілт бұзылған жағдайда, Тіркеу бөлімі кілттерді апаттық ауыстыру рәсімі аяқталғанға дейін осы кілтті пайдалануды жалғастырады.

5. ТЕХНИКАЛЫҚ ҚАУІПСІЗДІК ҚҰРАЛДАРЫ

5.1 Жасалған KSK кілттері желілік инфрақұрылымға қосылымы жоқ HSM (Hardware Secure Module – аппараттық қорғаныс модулі) деп аталатын арнайы құрылғыда жасалады және сақталады. Жабық KSK қатысуын талап ететін криптографиялық түрлендірулерді қолданатын барлық операциялар, сақтық көшірме ретінде пайдаланылатын осы құрылғыда немесе оған ұқсас құрылғыда орындалады. Қауіпсіздікті қамтамасыз ету үшін жабық KSK құрылғыдан тек шифрланған түрде шыға алады.

5.2 Жасалған ZSK кілттері жоғарғы деңгейлі домендер тізілімінің ішкі желісіне қосылған қол қою серверінде жасалады және сақталады. Жабық ZSK қатысуын талап ететін криптографиялық түрлендірулерді қолданатын барлық операциялар, сақтық көшірме ретінде пайдаланылатын осы құрылғыда немесе оған ұқсас құрылғыда орындалады. Қауіпсіздікті қамтамасыз ету үшін жабық ZSK құрылғыдан тек шифрланған түрде шыға алады.

5.3 Ашық KSK DNS протоколы арқылы қоғамдастыққа таратылады.
Параметрлерді орнату және негізгі ақпараттың сапасын тексеру тіркеу бөлімімен жүзеге асырылады.