DNSSECi juurutamise hea tava registripidajatele

Dokument on mõeldud registripidajatele ja nimeserveri teenuse pakkujatele, kes on huvitatud oma klientidele .ee domeeni tsoonis DNSSEC teenuse pakkumisest. Järgnev on mõeldud nõuannetena abistamaks teenusepakkujaid kvaliteetse teenuse pakkumisel.

Krüptoalgoritmid

EISi kodulehel on avaldatud .ee tsooni puhul kasutatavde võtmealgortimid ja parameetrid: http://internet.ee/et/dnssec/dnssec-eisis/

Teenusepakkuja võiks lähtuda ka oma võtmeparameetrite valikul neist väärtustest. Nõrgemad algoritmid muudavad teenusepakkuja DNSSEC usaldusahela nõrgimaks lüliks ja seega potentsiaalseks sihtmärgiks rünnetele. Oluliselt keerulisemad algoritmid nõuavad aga suuremat arvutusressurssi, kuid usaldusahela turvalisus tervikuna ei tõuse. EIS lähtub oma valikute tegemisel juurnimeserverites kasutatavatest parameetritest.

Kahe võtmepaariga lahendus

Soovitav on kasutada kahe võtmepaariga lahendust - ZSK ja KSK. ZSK ehk tsooni allkirjastamise võtmepaari kasutatakse konkreetse tsooni kirjete allkirjastamiseks. Seda võtit kasutatakse olenevalt tsooni suurusest ja kirjete arvust suhteliselt palju, mis tõttu on ressursi kasutuse seisukohalt mõttekas hoida seda võtit nii lühikesena kui võimalik. See omakorda tähendab, et võtit peab turvalisuse ja usaldusväärsuse tagamiseks suhteliselt tihti muutma. Et iga sellise muudatusega ei peaks kaasnema ka võtme muutmine .ee tsoonis, kasutatakse usaldusahela loomiseks teist võtmepaari - KSK ehk võtme kirjete allkirjastamise võti. KSK avalik osa on DNS kirjete õigsuse kontrollimiseks ning saadetakse EISi. Et seda võtmepaari harvem vahetada kasutatakse selle jaoks mahukamaid krüptoalgortime.

ZSK vahetus (*rollover) olgu regulaarne*

1024 bitise RSA-SHA256 ZSK võtmepaari soovitatav eluiga on 3 kuud kuni 1 aasta. EIS soovitab sellise pikkusega võtmeid vahetada vähemalt 2 korda aastas.

Kõik planeeritud ja regulaarsed võtmevahetused peaksid toimuma automaatselt.

Kasuta NSEC3

NSEC tagab, et ka päringud tsooni seal mitte eksisteerivate domeeninimede kohta saaksid allkirjaga kinnitatud vastuse. NSEC3 takistab selliste päringute abil tsooni faili sisu loetlemist.

NSEC3 parameetritena on soovitav kasutada ühte iteratsiooni 64bitise krüptograafilise soolaga, mille eluiga peaks olema sama, mis allkirjadel.

Dokumenteeri ja proovi läbi protseduurid

DNSSEC kaitseb hästi *man-in-the-middle* ja *dns cache poisoning* tüüpi rünnete vastu, kuid selleks vajalike võtmete haldus on täiendav kriitilise tähtsusega koht DNS süsteemis, millele

tuleb hoolega tähelepanu pöörata, sest viga seal võib tähendada, et kaitstud domeen(id) on ühtäkki suurele osale maailmast kättesaamatud.

Et seda vältida peavad olema valmis nii tavapärases olukorras võtmete haldamise ja vahetamise protseduurid kui ka tegutsemise plaan nö kriisisituatsioonis, kus DNSSECi usaldusahel on juba katki. Need on protseduurid, mida ei tehta igapäevaselt ja seetõttu on oluline, et need oleksid kirjalikus vormis ning selle järgi ka läbi testitud. Olulisimad protseduurid on:

- Võtmete regulaarne (tavapärases olukorras) vahetamine - ZSK ja KSK
- Võtmete vahetamine eriolukorras (rünne, süsteemi tõrge jne) - ZSK ja KSK
- Süsteemi taasteplaan

Avalda DPS (DNSSEC Practice Statement)

DPS on välja poole suunatud dokument, mis kirjeldab kuidas konkreetses organisatsioonis DNSSECi hallatakse. Dokumendi eesmärk on anda ülevaade kasutusel olevatest põhimõtetest, protseduuridest ja kordadest ning anda klientidele ja partneritele võimalus otsustada, kas nad usaldavad sellist lahendust.

DPS peaks olema avalikult kätte saadav organisatsiooni kodulehelt teenust tutvustavas osas.

Üks võti mitmele tsoonile või igale tsoonile oma

Samu võtmepaare saab kasutada samaaegselt mitme DNS tsooni jaoks. Küll aga tuleb silmas pidada, et sama võtmepaari kasutamisel mitmetes tsoonides muudab see võtmepaari kaalukamaks ründe sihtmärgiks ning võtmete kompromiteerumisel on tekkiv kahju suurem. Seetõttu tuleks pöörata võtmete laia kasutuse korral rohkem tähelepanu ka võtmete turvalisusele kasutades selleks näiteks spetsiaalset riistvaralist seadet - HSM (*Hardware Security Module*). Samal ajal võivad erinevad võtme kaitse lahendused seada omapoolseid piiranguid kasutatavate võtmete hulgale.

Registripidaja vahetus

Registripidajad ja DNSSEC teenuse pakkujad teevad omavahel koostööd kui klient on otsustanud teenusepakkujat vahetada. Et domeenile säiliks pidev DNSSECi kaitse on vajalik, et teenusepakkuja kelle juurest klient lahkub lisaks uue teenusepakkuja DNSSECi avaliku võtme oma tsooni olemasolevate võtmete kõrvale ning teenindaks domeeni DNS kirjeid seni kuni võib eeldada, et uue teenuspakkuja võtmed on jõudnud valdava enamuse lahendavate nimeserverite vahemälusse ehk peale võtme lisamist tsooni kuni kaks ööpäeva.

Vaata lisaks

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/networks-and-services-resilience/dnssec/gpgdnssec - Good Practices Guide for Deploying DNSSEC

http://tools.ietf.org/html/rfc6781 - DNSSEC Operational Practices, Version 2

http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-key-timing-03 - DNSSEC Key Timing Considerations

http://www.dnssec-deployment.org/documents/SettingtheParameters.pdf - DNSSEC▫ Operations: ▫Setting ▫the ▫Parameters

http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf - Secure Domain Name System (DNS) Deployment Guide

http://tools.ietf.org/html/rfc6841 - A Framework for DNSSEC Policies and DNSSEC Practice Statements