1. PIIRANGUD INFOMÜRA (SPÄMMI) KOHTA.

Võrgu areng on viinud selleni, et kasutajate peamiseks probleemiks on saanud info üleküllus. Seetõttu töötas võrguühendus välja spetsiaalsed eeskirjad, mis on mõeldud kasutajate kaitseks mittevajaliku/mittenõutud info (spämmi) eest. Näiteks ei ole lubatud järgmised toimingud.

1.1. Teadete massiline saatmine:

a) Teadete massiline saatmine elektronposti ja muude personaalsete infovahendite abil (k.a lühisõnumid nagu SMS, IRC jms), teisiti kui saaja selgel ja üheselt mõistetaval initsiatiivil.
b) Elektronposti aadressi või muu personaalse infovahetussüsteemi avalik publitseerimine ei ole põhjuseks aadressi lülitamiseks mingisse loendisse massiliste teadete saatmiseks.
c) Mis tahes viisil saadud aadressi (veebi, automaatse laialisaatmise süsteemi kaudu) lülitamist aadresside loendisse, mille alusel toimub mis tahes saatmine, lubatakse üksnes tingimusel, et on olemas sobiv tehniline protseduur allkirja kinnitamiseks, mis tagab, et aadress ei satuks loendisse muul viisil kui aadressi omaniku tahtel.
d) Allkirja kinnitamise protseduur peab välistama võimaluse, et aadress satub mingi laialisaatmiseks (ühekordseks või regulaarseks) ettenähtud aadresside loendisse kolmandate isikute initsiatiivil (s.t isikud, kes ei ole antud aadressi omanikud).
e) Igal tellijal (abonemendil) peab soovi korral olema võimalus ilma igasuguste takistusteta loendist lahkuda. Seejuures ei õigusta loendist lahkumise võimalus kui niisugune aadresside kandmist loendisse mitte aadresside omanike tahtel.

1.2. Manustega ja/või suuremahuliste elektronkirjade ja muude teadete saatmine ilma adressaadi eelneva loata.

1.3. Saata laiali (teisiti kui saaja otsesel initsiatiivil):

a) reklaami, kaubanduse või agitatsiooniga seotud elektronkirjad ja muud teated (k.a ühekordsed);
b) jõhkraid ja solvavaid väljendeid või ettepanekuid sisaldavad kirjad ja teated.
c) Teadete saatmine, mis sisaldavat palvet saata antud teade edasi teistele juurdepääsetavatele kasutajatele (chain letters).
d) Impersonaalsete („rolli") aadresside kasutamine teisiti kui aadressi valdaja ja/või standardite poolt määratud otstarbel.

Paigutada mis tahes elektronkonverentsi alla teateid, mis ei vasta antud konverentsi temaatikale (off-topic). Siin ja edaspidi mõistetakse konverentsi all telekonverentsi (uudistegruppi) Usenet ja teisi konverentse, foorumeid ja laialisaatmise loendeid.

1.4. Paigutada mis tahes konverentsi alla reklaamiga, kaubandusega ja agitatsiooniga seotud teateid, v.a juhul, kui antud konverentsi reeglid seda lubavad või kui nende paigutamine oli eelnevalt kooskõlastatud konverentsi omaniku või administraatoriga.
1.5. Paigutada mis tahes konverentsi alla artikleid, mis sisaldavad manuseid, v.a juhul, kui antud konverentsi reeglid lubavad manuseid või kui selline paigutamine oli eelnevalt kooskõlastatud konverentsi omaniku või administraatoriga.
1.6. Saata laiali infot saajatele, kes on varem selgelt väljendanud soovimatust saada seda infot, antud kategooria infot või antud saatja infot.
1.7. Kasutada isiklikke või saadaolevaid inforessursse (postkastid, e-posti aadressid, WWW leheküljed jt) kontaktkoordinaatidena mis tahes ülalnimetatud tegevusteks, sõltumata sellest, millisest võrgu punktist neid tegevusi sooritati.
1.8. Osutada tugiteenuseid spämmide laialisaatmiseks (spam support service), näiteks:

- inforessursside sisu sihipärane skaneerimine eesmärgiga koguda elektronposti ja teiste teadete kohaletoimetamise teenistuste aadresse;
- spämmide laialisaatmise tarkvara levitamine;
- luua, kontrollida, pidada või levitada elektronposti ja teiste teadete kohaletoimetamise teenistuste aadresside andmebaase (v.a juhul, kui kõik selles andmebaasis olevad aadresside omanikud on selgelt avaldanud nõusolekut aadressi lisamiseks antud konkreetsesse andmebaasi; see nõusolek ei taga aadressi avalikku publitseerimist).

2. MITTESANKTSIONEERITUD JUURDEPÄÄSU JA VÕRGURÜNNETE KEELD.

Keelatud on sanktsioneerimata juurdepääsukatsed võrguressurssidele, võrgurünnete teostamine ja võrku sissemurdmine ning nendes osalemine, v.a juhul, kui rünnet võrguressurssidele tehakse selle ressursi omaniku või administraatori selgesõnalisel loal. Sel juhul on keelatud:

2.1. Tegevused, mis segavad kasutajale mittekuuluvate võrguelementide (arvutid, muud seadmed või programmid) normaalset toimimist.
2.2. Tegevused võrguressurssidele (arvutitele, muudele seadmetele või inforessurssidele) mittesanktsioneeritud juurdepääsu saamiseks, selle juurdepääsu edasine kasutamine, samuti kasutajale mittekuuluva tarkvara või andmete hävitamine või muutmine ilma tarkvara omaniku või inforessursi administraatori nõusolekuta. Mittesanktsioneeritud juurdepääsu all mõeldakse igasugust juurdepääsu viisil, mis erineb sellest, mida ressursi valdaja eeldab.
2.3. Mõttetu või kasutu info edastamine arvutite või võrguseadmetega, mis koormab neid arvuteid või seadmeid ning võrgu vahelülisid mahus, mis ületab minimaalselt vajaliku mahu kontrollimaks võrkude sidusust ja juurdepääsu selle üksikutele elementidele.
2.4. Sihikindlad tegevused võrgusõlmede skaneerimisel eesmärgiga selgitada välja võrgu sisemine struktuur, avatud portide nimekiri jms erinevalt piiridest, mis on minimaalselt vajalik alaliste tehniliste meetmete läbiviimiseks, mille eesmärgiks ei ole käesoleva dokumendi punktide 2.1 ja 2.2 rikkumine.

3. RESSURSSIDE VALDAJA KEHTESTATUD JUHISTE JÄRGIMINE.

Võrgu mis tahes info- või tehnilise ressursi valdaja võib kehtestada sellele ressursile isiklikud kasutusjuhised.

- Ressursside valdajad või administraatorid peavad avaldama ressursside kasutuseeskirjad või viitama nendele ressursside sisselülituspunktis ning neid eeskirju peavad täitma kõik ressursside kasutajad.
- Eeskirjad peavad olema hõlpsasti kättesaadavad ning peavad arvestama kasutajate erinevat ettevalmistustaset.
- Valdaja kehtestatud ressursi kasutuseeskirjad ei tohi rikkuda teiste ressursivaldajate õigusi ega viia teiste ressursside kuritarvitamiseni.
- Kasutaja kohustub järgima ressursi kasutuseeskirju või siis keelduma kohe nende kasutamisest.
- Juhul kui ressursivaldaja kehtestatud eeskirjad on vastuolus käesoleva dokumendi ühe või teise punktiga, rakendatakse antud ressursi suhtes valdaja kehtestatud juhiseid, kui see ei vii rikkumiseni teiste ressursside suhtes.
- Juhul kui ressursside rühma valdaja poolt on eeskirjad kehtestatud ilmselt üksnes osale ressurssidest, siis ülejäänud ressursside puhul rakendatakse käesolevas dokumendis sõnastatud eeskirju.

4. VÕLTSIMISE MITTELUBAMINE.

Suur osa võrguressurssidest ei nõua kasutaja identifitseerimist ning lubab anonüümset kasutamist. Kuid mõnel juhul nõutakse kasutajalt teda identifitseerivate andmete esitamist ja tema poolt kasutatavaid vahendeid võrgule juurdepääsemiseks. Seejuures ei tohi kasutaja:

4.1. kasutada kolmandate isikute identifitseerimisandmeid (nimesid, aadresse, telefone jne.), v.a juhul, kui need isikud on andnud selliseks kasutuseks volituse;
4.2. võltsida oma IP-aadressi, samuti teistes võrguprotokollides kasutatavaid aadresse, kui ta esitab võrgule oma andmed;
4.3. kasutada elektronkirjade ja muude teadete saatmisel olematut tagasisaatmise aadressi.
4.4. suhtuda hoolimatult isiklike identifitseerimise rekvisiitide (sh paroolid ja muud pääsu lubavad koodid) konfidentsiaalsusesse, mis võimaldab kolmandatel isikutel kasutada teatud ressursse antud kasutaja nimel (varjates sel moel tegevuse tegelikku allikat).

5. ISIKLIKE RESSURSSIDE HÄÄLESTAMINE.

Töötades internetivõrgus saab kasutajast selle täieõiguslik osaleja, mis loob kolmandatele isikutele potentsiaalse võimaluse kasutajale kuuluvate võruressursside kasutamiseks. Seoses sellega peab kasutaja võtma ressursside häälestamiseks vajalikud meetmed, mis takistavad nende ressursside vastutustundetu kasutamise kolmandate isikute poolt, ning peab sellise kasutamise avastamisel võtma operatiivseid meetmeid sellise tegevuse lõpetamiseks.

Näited võrguressursside potentsiaalselt probleemsete häälestuste kohta:.

- elektronposti avatud retranslatsiooniseadmed (open SMTP-relays);
- lubamatuks avaldamiseks kõigile kättesaadavad uudisteserverid (konverentsi, gruppide);
- vahendid, mis võimaldavad kolmandatel isikutel ilma loata (lubamatul viisil) varjata ühenduse allikat;
- kõigile kättesaadavad kohalike võrkude leviaadresse, mille abil on võimalik teha smurf-tüüpi ründeid;
- laialisaatmise elektroonilised loendid, mille allkirja kinnitamise mehhanism ei ole piisavalt usaldusväärne või puudub võimalus selle tühistamiseks.;
- www-saidid ja muud sarnased ressursid, mis teostavad kirjade saatmist kolmandatele isikutele vastavalt nõuetele, mis on anonüümsed või mille algupära ei ole piisavalt tõestatud.

Ref.: www.ofisp.org

AS INFONET, REG. NR. 10096260, KMKR EE1001964031
SUURTÜKI 8, 10412 TALLINN, ESTONIA, PHONE: (372) 640 0000, FAX: (372) 640 0064, E-MAIL: INFO@INFONET.EE, HTTP://INFONET.EE
SWEDBANK, LIIVALAIA 8, 15040 TALLINN, ESTONIA, ACCOUNT No. 221001184160, IBAN: EE632200221001184160, SWIFT/BIC: HABAEE2X