Exp 10/12-02

LINKÖPINGS UNIVERSITET
Vicerektor för IT-frågor

BESLUT
2002-12-03

Dnr LiU 1689/02-14

Åtgärder för ökad IT-säkerhet: Epostservrar

Massutsända, oönskade brev över Internet, så kallad spam, är ett ständigt ökande problem. Primärt ur ett centralt perspektiv är att befintliga servrar inte används som mellanhand, så kallad relä vid spamutskick, då detta kan leda till svartlistning, problem att sända epost till andra, och allmänt dåligt rykte för universitetet. Ur ett användarperspektiv är den egna volymen inkommande spam det primära.

För att minska effekten av spam gäller följande för all eposthantering inom LiU:s nätverk:

Central resurs för läsning och sändning av epost
Alla anställda och studerande inom Linköpings universitet skall erbjudas epostkonto inom ramen för centrala IT-tjänster. Såväl läsning och sändning sker via nyttjande av gemensamt epostsystem. Avtal om förvaltning och drift tecknas av universitetsledningen.

Institutioner och enheter som själva önskar administrerar anställdas epost kan ta emot och sända epost genom egen server.

Följande nivåer kan förekomma:
Egen epostserver för institution eller enhet, ej nåbar utifrån.
Epostserver som ej är direkt nåbar utifrån skall meddelas Incident Response Team (IRT) för godkännande och identifiering i den centrala epostfunktionen.

Egen epostserver, direkt nåbar utifrån.
För att vara direkt nåbar utifrån skall servern godkännas av IRT. Endast en server tillåts om inte särskilda skäl föreligger. Vid godkännande läggs stor vikt vid hantering av reläande, men även övrig kompetens att sköta en epostserver.
Den centrala nätverksutrustningen är konfigurerad så att enbart godkända servrar är direkt nåbara utifrån.

För samtliga epostservrar gäller att:
- Servrar skall vara i "gott skick", d v s alla relevanta säkerhetsuppdateringar skall vara installerade och maskinerna skall ha relevanta accesskydd.
- Serverprogramvaran skall uppfylla relevanta Internetstandarder för elektronisk posthantering, se http://www.ietf.org/rfc.html.
- Se även Åtgärder för ökad IT-säkerhet: säkerhet för enskilda datorsystem.

För epostservrar direkt nåbara utifrån gäller dessutom:
- Serverprogramvaran skall ha aktiverade skydd mot reläande och bör vara försedd med spamfilter.

Ovanstående skall kontinuerligt hållas aktuellt. Epostservrar som inte uppfyller kraven kan få godkännandet tillbakadraget och bli avstängda.

Administratörer av epostservrar förväntas delta i samarbete kring datordrift (epostlistor och möten mm).

Mille Millnert
Vicerektor för IT-frågor

Gun Djerf
IT-säkerhetschef

Delges:
Institutionerna
Övriga enheter
Rektorskansliet (Djerf, Hessling, C Karlsson, Tegnefur)
De lokala fackliga organisationerna
Centrala säkerhetsgruppen för IT-frågor
Centrala nätverksgruppen