Livelli di sicurezza, livelli minimi di servizio e standard per l'erogazione dei servizi di posta elettronica

(ai sensi dell'art. 8 del "Regolamento di utilizzo dei servizi di comunicazione")

Premesso che i server di posta elettronica sono soggetti alla normativa vigente ed in particolare:

a) al Decreto legislativo 30 giugno 2003, n.196 "Codice in materia di protezione dei dati personali";
b) al Regolamento di "attuazione del codice di protezione dei dati personali in possesso all'Università di Firenze" emanato con D. R. del 7 luglio 2004, n.449, che prevede l'emanazione, entro termini stabiliti dal Codice, del Documento Programmatico della Sicurezza da parte del responsabile dell'unità amministrativa, titolare dei dati personali da essa detenuti;
c) alle Regole di Accesso e di Utilizzo della Rete del GARR;
d) al Regolamento di utilizzo dei Servizi di Comunicazione emanato con D. R. del 1 settembre 2004, n.657;

Art. 1 – Ambito di applicazione

Il presente documento disciplina le modalità e i termini per l'erogazione dei servizi di posta elettronica nell'Università degli Studi di Firenze. Esso definisce gli standard e i livelli minimi obbligatori di servizio e di sicurezza che devono essere implementati sui server di posta elettronica installati presso l'Università di Firenze.

Il documento si applica allo CSIAF e alle unità amministrative che detengono i server di posta elettronica ammessi dal "Regolamento di utilizzo dei servizi di comunicazione".

Art. 2 – Responsabilità

I server di posta elettronica presso le unità amministrative ricadono operativamente ed amministrativamente sotto il responsabile dell'unità amministrativa medesima.

Il responsabile dell'unità amministrativa può nominare un "referente tecnico" del servizio fra il personale strutturato afferente all'unità amministrativa.

Art. 3 – Requisiti minimi per l'hardware e il software di sistema

I server atti ad ospitare i servizi di posta elettronica devono garantire:

1. la continuità del servizio, da attuarsi mediante
    a. gruppo di continuità con capacità di almeno 1 ora di funzionamento,
    b. contratto di manutenzione hardware con tempi di intervento inferiori o uguali a 8 ore lavorative,

    o misure equivalenti;
2. livelli di sicurezza adeguati da attuarsi mediante
    a. aggiornamento all'ultima release disponibile del sistema operativo,
    b. backup/restore con cadenza almeno settimanale,
    c. collocazione del server in un locale chiuso con accesso controllato.

Art. 4 – Requisiti minimi per il software di posta elettronica

I server atti ad ospitare i servizi di posta elettronica devono:

1. utilizzare il protocollo standard smtp [1];
2. filtrare i messaggi di posta con software antivirus costantemente aggiornato;
3. disporre di software aggiornato all'ultima release disponibile;
4. impedire l'uso come relay dall'esterno del dominio, ad eccezione dei server che utilizzano l'estensione ESMTP AUTH (autenticazione del mittente per la spedizione) o meccanismi alternativi (POP before SMTP) [2];
5. ospitare una casella "postmaster" e di una casella "abuse" per ogni dominio di posta gestito [3];
6. ospitare gli indirizzi di funzione sui domini conformemente a quanto indicato nel "Regolamento di utilizzo dei servizi di comunicazione".

Art. 5 – Misure adottate

Ai server che soddisfano quanto specificato nei precedenti articoli 3 e 4 viene consentito il passaggio attraverso le apparecchiature di rete del traffico inerente ai protocolli relativi alla posta elettronica, previa presentazione allo CSIAF della dichiarazione in allegato; l'accesso alla rete viene mantenuto a condizione che la gestione si mantenga conforme ai requisiti richiesti. Per tutti gli altri server il passaggio dei protocolli inerenti alla posta elettronica viene inibito.

Ogni abuso commesso mediante il server, che venga rilevato o segnalato allo CSIAF, o la diffusione, anche inconsapevole, di virus, determinerà il blocco del traffico inerente ai protocolli relativi alla posta elettronica sulle apparecchiature di rete, in via cautelare temporanea o permanente a seconda del danno o disservizio arrecato, secondo la procedura specificata all'art. 3 del "Regolamento dei servizi di comunicazione".

Art. 6 – Raccomandazioni

Nell'ottica della migliore erogazione del servizio e, soprattutto, della sicurezza dei server di posta elettronica si raccomanda:

1. l’uso di un firewall. Il server di posta elettronica dovrebbe essere protetto da un firewall che espone per il server solo le porte dei protocolli necessari per l’erogazione del servizio; alternativamente, in mancanza di firewall, il server dovrebbe essere configurato in modo da esporre solo le porte di cui sopra.
2. la ridondanza. Dipendentemente dal bacino di utenza e dal traffico il servizio di posta dovrebbe essere installato su server in cluster (almeno due macchine che erogano il servizio) o, alternativamente, su hardware ridondante.

Art. 7 – Interazione con CSIAF

- in base al "Regolamento di utilizzo dei servizi di comunicazione" lo CSIAF deve creare le caselle di posta elettronica per tutto il personale nella forma **nome.cognome@unifi.it;** lo CSIAF può reindirizzare (forward) il traffico verso le caselle di posta dei server a gestione autonoma a coloro che ne facciano richiesta.

Riferimenti

[1] – RFC 2821, “Simple Mail Transfer Protocol”, April 2001 (e sue estensioni e aggiornamenti)

[2] – RFC 1939, “Post Office Protocol – Version 3”, May 1996 (e sue estensioni e aggiornamenti)

[3] - RFC 2142 “Mailbox Names for Common Services, Roles and Functions” , maggio 1997

Allegato A – Dichiarazione di responsabilità

Il sottoscritto …in qualità di responsabile dell'Unità Amministrativa …

dichiara

- che il server di posta elettronica xxx.xxx.unifi.it con indirizzi IP 150.217.xxx.xxx, configurato per la gestione dei domini di posta elettronica xxx.unifi.it e xxx.unifi.it:

- era in funzione alla data del 15 settembre 2004.

- risponde pienamente ai requisiti minimi previsti dagli artt. 3 e 4 del documento "Livelli di sicurezza, livelli minimi di servizio e standard per l'erogazione dei servizi di posta elettronica " predisposto dallo CSIAF.

- che soddisfa anche i seguenti ulteriori requisiti di servizio e di sicurezza:

…….
…….
.

Il sottoscritto dichiara inoltre di aver preso visione di tutto quanto descritto nel predetto documento predisposto dallo CSIAF e [comunica che il responsabile tecnico del servizio di posta è …….. (opzionale)]