UNITN|30/06/2014|0013473|P - Allegato Utente 1 (A01)

UNIVERSITÀ DEGLI STUDI
DI TRENTO

Direzione Sistemi Informativi, Servizi e Tecnologie Informatiche

Regole Operative
del
sistema Anti-Virus e Anti-Spam (AVAS)
per la posta elettronica di Ateneo

Versione 2.0
30 giugno 2014
Direzione Sistemi Informativi, Servizi e Tecnologie informatiche

Via Briamasco, 2 - Palazzina S.I.S.T.I., - 38123 Trento, Italy
Tel. +39 0461 281228, Fax +39 0461 281162 e-mail:dir.sisti@unitn.it

1. Obiettivi

1.1. Le presenti regole operative disciplinano la gestione e l'uso del sistema Anti-Virus e Anti-Spam (AVAS) per il servizio di posta elettronica di Ateneo gestito dalla Direzione Sistemi Informativi, Servizi e Tecnologie Informatiche.

1.2. Il sistema AVAS mira a preservare l'efficienza e l'efficacia della posta elettronica di Ateneo tramite:

- Il filtro automatico dei messaggi spam o infetti da software malevolo a livello di frontiera della rete di Ateneo;
- La rimozione dai messaggi infetti del software malevolo;
- La cancellazione o l'invio con marcatura dei messaggi spam;
- Il blocco automatico di invii massivi di messaggi, se non preventivamente comunicati, da parte di un indirizzo mittente al superamento di limiti massimi predefiniti, al fine di ridurre i rischi di 'spamming' e/o 'blacklisting' del sistema di posta elettronica di Ateneo a seguito di attacchi di 'phishing' rivolti agli utenti;
- La riduzione del carico di lavoro dell'utente e l'ottimizzazione dell'uso delle risorse informatiche e telematiche dell'Ateneo.

2. Ambito di applicazione

2.1. Il sistema AVAS (http://icts.unitn.it/avas-antivirus-e-antispam) è applicato a tutti gli indirizzi di posta elettronica d'Ateneo dipendenti dai domini UNITN.IT e UNITN.EU che comprendono:

- Indirizzi di posta elettronica del personale dipendente, collaboratori ed ospiti;
- Indirizzi di posta elettronica istituzionale delle strutture di Ateneo;
- Liste di distribuzione.

2.2. Il sistema AVAS può essere applicato, sulla base di una richiesta di adesione presentata alla Direzione Sistemi Informativi, Servizi e Tecnologie Informatiche all'indirizzo dir.sisti@unitn.it,ad altri domini postali, oltre quelli sopra indicati anche esterni all'Ateneo, nell'ambito della comunità locale della ricerca e istruzione universitaria. L'utilizzo del sistema AVAS comporta la piena accettazione delle presenti regole operative.

2.3. Il servizio di posta elettronica degli studenti, individuato dal dominio STUDENTI.UNITN.IT, è basato sull'utilizzo di un indirizzo di posta elettronica privato ed esterno all'Ateneo indicato dallo studente nella fase di immatricolazione. Tale servizio è dotato di un proprio e distinto sistema anti-virus e anti-spam che non è oggetto delle presenti regole operative ma persegue finalità simili e adotta regole analoghe.

3. Regole Operative

3.1. Filtro e classificazione dei messaggi di posta elettronica

3.1.1. Sulla base di proprie regole interne il sistema AVAS filtra automaticamente i messaggi di posta elettronica in entrata e in uscita classificandoli in una delle seguenti categorie:

- Messaggi infetti da software malevolo;

- Messaggi 'spam';
- Messaggi 'sospetto spam';
- Messaggi legittimi.

3.2. Messaggi in entrata

3.2.1. Ai messaggi in entrata sono applicate le seguenti regole:

- I messaggi legittimi sono recapitati al/ai destinatario/i.
- I messaggi con file allegati potenzialmente eseguibili (es. file con estensione .exe, .cmd, .bat, .zip, etc.) sono recapitati al/ai destinatario/i con l'aggiunta nel corpo del messaggio di un avviso relativo alla presenza di un allegato potenzialmente eseguibile; i messaggi con file allegati che la componente Anti-Virus del sistema AVAS non è stata in grado di analizzare sono recapitati al/ai destinatario/i con l'aggiunta nel corpo del messaggio di un avviso relativo alla presenza di un allegato che non è stato possibile analizzare.
- I messaggi infetti da software malevolo sono marcati nel campo oggetto con l'etichetta 'ATI-Network: VIRUS DETECTED' e, dopo la rimozione del software malevolo, sono recapitati al/ai destinatario/i.
- I messaggi classificati 'spam' sono automaticamente cancellati.
- I messaggi classificati 'sospetto spam' sono marcati nel campo oggetto con l'etichetta 'ATI-Network: probabile SPAM' e recapitati al/ai destinatario/i.

3.2.2. Con l'obiettivo di migliorare le prestazioni del sistema AVAS, l'utente può segnalare all'indirizzo network@unitn.it i messaggi:

- FP o Falso Positivo, cioè il messaggio legittimo classificato 'sospetto spam';
- FN o Falso Negativo, cioè il messaggio spam erroneamente classificato legittimo.

3.3. Messaggi in uscita

3.3.1. Ai messaggi in uscita sono applicate le seguenti regole:

- I messaggi legittimi sono inviati al/i destinatario/i;
- I messaggi infetti da software malevolo sono automaticamente cancellati;
- I messaggi classificati 'spam' o 'sospetto spam' sono automaticamente cancellati. Se il mittente del messaggio è un indirizzo di posta elettronica appartenente ai domini di cui ai punti 2.1 e 2.2, viene inviato un avviso al mittente medesimo di messaggio non recapitato;
- In presenza di invii massivi di messaggi da parte di un indirizzo mittente che superano i limiti massimi predefiniti, i messaggi stessi sono bloccati e cancellati. Inoltre l'indirizzo mittente e l'account ADA dell'utente associato sono bloccati.
  Le misure applicate agli invii massivi di messaggi di posta elettronica sono indicati al successivo punto 3.3.2.

3.3.2. Misure applicate agli invii massivi di messaggi da parte di un indirizzo mittente al fine di ridurre i rischi di 'spamming' e/o 'blacklisting' del sistema di posta elettronica di Ateneo a seguito di attacchi di 'phishing' (http://icts.unitn.it/limiti-invio-messaggi-posta-elettronica):

- La tabella seguente elenca i limiti predefiniti al numero massimo di messaggi inviati nell'intervallo di tempo da parte di un indirizzo mittente:

Numero Massimo di Messaggi Inviati	Intervallo di Tempo
250 messaggi	5 minuti
500 messaggi	15 minuti
1.000 messaggi	30 minuti
2.500 messaggi	60 minuti

- Al superamento dei limiti predefiniti segnalato automaticamente dal sistema AVAS i messaggi sono bloccati e cancellati. Inoltre l'indirizzo mittente e l'account ADA dell'utente associato sono bloccati ed il servizio Computer Emergency Response Team (CERT) della Direzione informa il servizio utenti di polo dell'utente.
- In presenza di una potenziale compromissione di un indirizzo di posta elettronica, anche non segnalata dal sistema AVAS, il personale tecnico della Direzione Sistemi Informativi, Servizi e Tecnologie Informatiche, può in ogni caso intervenire bloccando manualmente l'indirizzo e l'account ADA dell'utente associato.
- L'indirizzo e l'account ADA bloccati sono sbloccati - su richiesta dell'utente interessato presentata al servizio utenti di polo (http://icts.unitn.it/servizi-utente-di-polo) - a seguito di idonee verifiche tecniche, di una effettiva sensibilizzazione dell'utente sui rischi connessi al fenomeno del 'phishing' e con l'autorizzazione del Dirigente della Direzione Sistemi Informativi, Servizi e Tecnologie informatiche.
- E' attivo un servizio di 'whitelisting' che permette agli utenti di richiedere preventivamente l'abilitazione di uno specifico indirizzo all'invio massivo di messaggi; la richiesta va presentata attraverso il sistema di HelpDesk informatico http://servicedesk.unitn.it o inviata all'indirizzo network@unitn.it. Per gli indirizzi istituzionali delle strutture di Ateneo è possibile richiedere una abilitazione permanente, mentre per gli indirizzi del personale dipendente, collaboratori o ospiti è prevista una abilitazione limitata ad un intervallo temporale che deve essere specificato nella richiesta.