Università degli Studi di Udine

Modalità e limiti di utilizzo della rete telematica dell'Università di Udine

Gruppo di lavoro istituito il 16 aprile 2004 con decreto rettorale n. 281
Pier Luca Montessoro, Francesco Savonitto, Claudio Castellano, Fabio Romanelli

Premessa

L'accentuarsi delle attività illecite in Internet ha reso anche la rete dell'Università di Udine sempre più frequentemente oggetto di attacchi dall'esterno e di usi impropri o illegali dall'interno. Le conseguenze dal punto di vista tecnico vanno dalla riduzione delle funzionalità alla perdita o alterazione dei dati, ma ben più preoccupanti sono le implicazioni di tipo giuridico per gli amministratori e i responsabili di sistemi.

Il gruppo di lavoro istituito con il decreto rettorale n. 281 del 16.04.2004, nel corso della sua attività, ha raccolto ed analizzato documentazione relativa ad aspetti tecnici e giuridici, ha confrontato esperienze interne ed esterne all'Ateneo ed ha infine definito le linee guida nel seguito riportate.

Alla luce delle recenti normative, sia in ambito civile che penale, sono state individuate tre linee di azione fondamentali in materia di responsabilità e sicurezza nell'uso e nella gestione della rete:

1. Responsabilizzazione dell'utente[1]: ogni utente della rete di Ateneo è responsabile delle proprie azioni ed è tenuto ad utilizzare la rete nel rispetto delle vigenti regole del GARR e delle vigenti leggi; è inoltre tenuto a rispettare le raccomandazioni tecniche sulla sicurezza informatica emanate dall'Ateneo;
2. Politica di aggiornamento dei sistemi informatici degli utenti e di gestione sistemistica degli stessi mediante interventi diretti (amministrazione) o raccomandazioni tecniche interne (didattica e ricerca);
3. Gestione delle segnalazioni di azioni illecite perseguibili sia in sede amministrativa, che penale, che, eventualmente, disciplinare: dovrà essere istituito un gruppo permanente di gestione delle emergenze che possa avviare tempestivamente le necessarie azioni tecniche e formali, incluse le comunicazioni alle autorità competenti, ora obbligatorie per legge.

Nel seguito vengono illustrate in maggior dettaglio tali linee di azione e sono riportate le relative raccomandazioni tecniche ed organizzative.

1. Responsabilità dell'utente

La responsabilizzazione degli utenti della rete è strumento indispensabile onde prevenire gli usi impropri o illegali e quelle azioni che rendono vulnerabili i sistemi.

L'utente è tenuto a rispettare le raccomandazioni tecniche sul comportamento degli utenti in materia di sicurezza informatica emanate dall'Ateneo. In particolare, è tenuto a rispettare scrupolosamente le seguenti indicazioni.

Finalità della rete di Ateneo

[1] Per "utente" si intende ogni utilizzatore (personale, strutturato e non, studenti e terzi qualificati per tali finalità) della rete e dei sistemi informatici disponibili presso l'Università.

La rete di Ateneo dell'Università degli Studi di Udine è a disposizione dell'utenza esclusivamente per le attività didattiche e scientifiche ed amministrative. Gli strumenti informatici, compresa la posta elettronica, messi a disposizione del personale, strutturato e non, degli studenti e di terzi qualificati per tali finalità, sono affidati alla loro custodia personale, dal momento della loro consegna o comunque all'atto del loro utilizzo.

Accesso agli elaboratori e ai servizi di rete

Tutti i sistemi informatici, e in particolare quelli collegati in rete, dovranno essere provvisti di sistema di autenticazione. È responsabilità dell'utente conservare e non divulgare la propria password o il proprio dispositivo di autenticazione (es. smartcard) e scegliere password non banali (quali il proprio nome, la propria data di nascita, la password predefinita, parole ovvie quali "password", ecc.) così come previsto dalle norme vigenti.

Utilizzo del proprio computer, del proprio account e della propria casella di posta elettronica.

L'utente è tenuto a custodire il PC (se affidatogli in uso), il proprio account e la propria casella di posta elettronica come tutti gli altri strumenti che gli vengono consegnati dall'Università per svolgere le proprie mansioni o attività. L'utente è tenuto a non rendere pubblicamente (ovvero senza alcuna protezione) disponibili via rete i dati residenti sul proprio computer o sul proprio account, per esempio abilitando la condivisione dei dischi.

Installazione di programmi sul proprio computer

L'utente è tenuto a non installare software non esplicitamente autorizzato e certificato dall'amministrazione. Fanno eccezione gli amministratori di sistemi informatici didattici e scientifici, inclusi quindi personal computer di docenti e ricercatori, che sono responsabili dei programmi installati su tali sistemi e sugli eventuali danni (per esempio in termini di violazione della sicurezza di altri sistemi) che essi possono provocare. Ogni applicazione o file ritenuti pericolosi dall'Amministrazione verranno eliminati.

Utilizzo di servizi della rete Internet

L'utente è tenuto a non utilizzare servizi di rete in violazione delle vigenti leggi, con particolare riferimento al diritto d'autore, terrorismo, pedopornografia.

2. Gestione dei sistemi

L'aumento del livello di sicurezza nell'uso della rete e la tutela dei sistemi nei confronti di attacchi esterni, che possono far figurare la rete dell'Università di Udine come sorgente di ulteriori attacchi e violazioni, richiedono inevitabilmente un progressivo e continuo aggiornamento dei sistemi informatici. Questo può essere perseguito solo mediante una politica che affianchi adeguati investimenti a procedure organizzative efficaci.

Gestione tecnica

È necessario distinguere due tipologie di sistemi:

- computer per amministrazione
- computer per didattica o della ricerca

Nel primo caso, infatti, la gestione deve essere centralizzata, ad opera dello CSIT (Centro Servizi Informatici e Telematici), e i relativi personal computer devono essere progressivamente resi più sicuri, limitando e possibilmente eliminando l'accessibilità dell'utente alle configurazioni del sistema.

Nel secondo caso, invece, la gestione tecnica è tipicamente delegata al docente, al ricercatore o al personale tecnico di supporto alla didattica e alla ricerca, e le finalità di tali sistemi mal si conciliano con una politica rigorosa di controllo e di "blindatura". È pertanto necessario che vengano emanate delle raccomandazioni tecniche, ad opera dello CSIT, che fungano da guida per una gestione autonoma e conforme a criteri minimi di sicurezza.

A titolo di esempio, si cita la necessità di mantenere aggiornati i sistemi operativi e i sistemi antivirus mediante aggiornamenti automatici on-line, anche in conformità alle vigenti disposizioni di legge in materia di gestione dei sistemi informatici per il trattamento di dati personali o dati sensibili.

Inoltre, non deve essere consentita l'attivazione di postazioni di lavoro o di punti informativi per il pubblico non presidiati con accesso non autenticato alla rete di Ateneo.

Monitoraggio delle attività

Nel pieno rispetto delle norme che disciplinano il rapporto di lavoro e delle vigenti disposizioni in materia di privacy, nella normale attività di gestione della rete potranno essere effettuati controlli e monitoraggi sul traffico di rete, in modalità anonima (nel senso che risulti soltanto il destinatario dell'accesso - per esempio l'indirizzo della pagina web - e non il computer o l'utente che l'ha richiesto), per verificare quali siano i servizi di rete più utilizzati e i siti più frequentemente visitati e che i medesimi siano compatibili con le attività istituzionali dell'Ateneo.

È tuttavia possibile che nel corso di operazioni di manutenzione gli operatori vengano a conoscenza, in modalità non anonima, di accessi a siti e servizi.

Si tiene a precisare che l'amministrazione non effettuerà in alcun modo verifiche sul contenuto, ad esempio, dei singoli messaggi di posta elettronica; tuttavia è garantita la riservatezza esclusivamente dei dati personali censiti dall'amministrazione centrale e memorizzati all'interno dei database dell'Ateneo oppure trasferiti sulla rete mediante accessi crittografati predisposti dall'Ateneo. Ogni altra forma di memorizzazione o trasferimento di dati personali avviene sotto la responsabilità dell'utente che la attua e non è tutelata dall'Università degli Studi di Udine.

3. Gruppo permanente di gestione delle emergenze

Sono ormai frequenti le segnalazioni di illeciti effettuati su computer della rete di Ateneo e rilevati da enti esterni ad essa. Le vigenti leggi impongono anche all'Università la comunicazione di tali attività alle autorità competenti.

Per poter verificare e valutare le circostanze in cui tali eventi avvengono, nonché coordinare le azioni da intraprendere e curare i rapporti con le autorità competenti, è necessario istituire un gruppo permanente di gestione delle emergenze. Tale gruppo dovrebbe essere composto dagli stessi soggetti autori del presente documento più un rappresentante dell'utenza scientifica e didattica, in qualità di:

- Responsabile amministrativo del polo GARR dell'Università degli Studi di Udine
- Responsabile tecnico del polo GARR dell'Università degli Studi di Udine
- Direttore Amministrativo
- Responsabile Centro Legale e Affari Istituzionali
- Rappresentante dell'utenza scientifica e didattica nominato dal Senato Accademico

Tutte le segnalazioni di violazioni della sicurezza, attività illecite, ecc. dovranno essere inoltrate a questo gruppo di gestione delle emergenze che provvederà a:

- Raccogliere i dati e le informazioni relative all'evento segnalato, provvedendo ove possibile a far effettuare copie di file dati e di file di log potenzialmente utili per successive indagini;
- Analizzare le circostanze dell'evento, distinguendo tra violazioni provenienti dall'esterno ad insaputa del gestore del sistema e violazioni effettuate a seguito di attività esplicita e volontaria dell'utente;
- Segnalare, in modo differenziato, gli eventi alle autorità competenti. In particolare:
    - Per le violazioni provenienti dall'esterno ad insaputa del gestore del sistema, si indicheranno i dati tecnici relativi al sistema violato e le contromisure adottate;
    - Per le violazioni volontarie, si indicheranno le circostanze segnalate e i dati tecnici raccolti.

4. Interventi in caso di rilevamento di irregolarità

Nell'ipotesi in cui venga rilevata una delle seguenti situazioni:

- elaboratore che svolge attività illecite;
- elaboratore che genera in ingresso/uscita traffico eccessivo;
- elaboratore compromesso da virus, worm, etc.

i gestori della rete di Ateneo sono autorizzati a disabilitare l'accesso in rete di tale elaboratore fino a quando non verrà eliminata la condizione di compromissione della sicurezza.

5. Conclusioni

Il presente documento ha individuato gli elementi ritenuti essenziali per un corretto e responsabile uso ed una efficace gestione della rete di Ateneo.

Il presente documento sarà posto al parere del Senato Accademico (anche ai fini della designazione del Rappresentante dell'utenza scientifica e didattica nel Gruppo permanente di gestione delle emergenze) e all'approvazione del Consiglio di Amministrazione. Successivamente sarà emanato con decreto rettorale al fine di conferirgli data certa e infine sarà comunicato a tutti i responsabili delle strutture dell'Ateneo.

Si suggerisce inoltre, in un secondo tempo, magari alla luce di una prima sperimentazione delle procedure di gestione delle emergenze sopra descritte, di redigere un regolamento dettagliato sull'utilizzo e sulla gestione della rete, analogamente a quanto è stato fatto in altri atenei (alcuni esempi sono riportati in allegato).

6. Elenco allegati

1. Documento "Acceptable User Policy" della rete GARR
2. Estratto del Decreto Legislativo 22 marzo 2004, n. 72
3. Estratto del Decreto Legislativo 9 aprile 2003, n. 70
4. Estratto Legge 22 aprile 1941 n 633 sul diritto d'autore
5. Regolamento di accesso ai servizi di rete dell'Università degli Studi di Parma
6. Regolamento per l'accesso al sistema integrato di reti dell'ateneo di Trieste

7. Regolamento (CE) n. 460/2004 istitutivo dell'Agenzia europea per la sicurezza delle reti e dell'informazione
8. Articolo 'Internet e azienda', inserto di 'Diritto e pratica del lavoro' del n, 1/2002