



POLITECNICO DI TORINO

C.so Duca degli Abruzzi, 24 - 10129 TORINO (Italia)
Tel. + 39. 011. 564.6302 - Telefax + 39. 011. 564.6399 - email: prorettore@polito.it

IL PRO RETTORE

Prot. n° 058.070203

Torino, 07-02-2003

A tutto il personale

OGGETTO: **Sicurezza Informatica e Virus "Sapphire"**

Come è noto, nella scorsa settimana un codice virale, identificato come "**W32 Slammer**", "**Worm Sapphire**" o "**SQ-Hell**" ha attaccato la rete internet. Partito presumibilmente dal far east, ha bloccato numerosissimi siti aziendali a livello mondiale, anche di significativa dimensione, procurando notevoli danni e sensibili disagi, in particolare l'impossibilità di accesso a servizi di rete sia interni che esterni.

La rete del Politecnico è molto vasta, non totalmente omogenea e su di essa non è possibile stabilire rigorose politiche di sicurezza che imporrebbero un rigido governo e controllo centralizzato su tutte le postazioni, sulla loro configurazione e sugli apparati di rete. Tale situazione, strutturale in considerazione della natura "aperta" di una organizzazione quale è l'Università, può determinare intrinsecamente maggiori debolezze nei confronti di attacchi o reati informatici sia dall'esterno che dall'interno dell'Ateneo. Di questo tutti ne devono essere coscienti e deve indurre i singoli a comportamenti più marcatamente attenti e responsabili.

In relazione al citato attacco virale della scorsa settimana, voglio rendere noto a tutti il grande senso di responsabilità e disponibilità del personale del Ce.S.I.T. e dei referenti informatici delle strutture autonome dell'Ateneo (Dipartimenti, Centri, ecc.) che con il loro impegno, già da venerdì 24 sera e poi durante le giornate di sabato 25, domenica 26 e lunedì 27 gennaio, hanno permesso di bloccare gli effetti del worm informatico creando solo lievi disagi al Politecnico nella giornata del 27.

Voglio ricordare a tutti che le situazioni critiche nell'uso dei sistemi informatici stanno crescendo in modo rilevante all'interno dell'Ateneo. E' quindi sempre più frequente che il Politecnico (tramite il CeSIT), la Procura della Repubblica e gli organi di Polizia si debbano adoperare in azioni connesse a situazioni che si possono identificare come violazioni delle vigenti leggi in materia di crimini informatici e che hanno portato, da parte mia in alcuni casi, ad esplicita querela anche nei confronti di soggetti direttamente o indirettamente appartenenti all'Ateneo.

E' stato costituito a tal fine nel CeSIT, già dagli inizi dell'anno scorso, un **nucleo per la Sicurezza Informatica** con visibilità su tutto il sistema informatico dell'Ateneo e con funzioni anche mirate al monitoraggio, auditing e rilevazione di situazioni potenzialmente critiche. Tale nucleo opera stabilmente e collabora con gli organi istituzionali preposti alla sicurezza informatica e telematica.

Tenuto conto della finalità di una istituzione come la nostra che impone attenzione alla realizzazione di una politica di sicurezza non troppo rigida, come invece la maggior parte degli enti esterni realizza, si vogliono qui ricordare le responsabilità, che hanno risvolti diretti



sul piano giuridico anche penale, dei gestori di sistemi di elaborazione, i quali devono attuare, anche sulla base della normativa vigente, tutte quelle azioni tecniche ed organizzative atte a garantire un funzionamento “sicuro” del sistema.

Si sottolinea peraltro come le principali situazioni critiche che si verificano siano, nella maggioranza dei casi, riconducibili a utilizzi personali non appropriati dei servizi informatici dell'Ateneo da parte di utilizzatori/assegnatari che si richiamano quindi alla massima responsabilità.

A titolo informativo si ricorda che, nel corso del 2002 il CeSIT ha effettuato oltre 30 segnalazioni di criticità in termini di sicurezza informatica. Tra queste si segnalano in modo particolare, anche a causa del crescente utilizzo di software “peer to peer” per lo scambio e condivisione di file (Gnutella, Kazaa, Morpheus, WinMX, Gnucleus, AudioGnome,) quelle relative a materiale audio e video protetto dal diritto d'autore. In particolare, con specifico riferimento a questa tipologia di criticità, si sottolinea come, oltre ad eventuali comportamenti illegali riconducibili direttamente al responsabile della postazione, lo scorretto utilizzo delle dotazioni di Ateneo può procurare nocimento al corretto funzionamento della rete e quindi dei servizi informatici e può pertanto configurarsi come danneggiamento di bene di utilità pubblica.

Anche in considerazione della rilevanza che la materia della sicurezza informatica assume nella quotidiana attività lavorativa svolta dal personale attraverso gli strumenti informatici, il CeSIT intende realizzare prossimamente un ciclo di conferenze mirato ad illustrare aspetti giuridici, potenziali rischi, responsabilità civili e penali personali e dei gestori di sistemi, modalità comportamentali a tutela personale e dell'istituzione.

Riferimenti CeSIT per segnalazioni:

Ce.S.I.T. - ICT Security

Telefono: **011-5646693**

E-Mail: **CeSIT.ICTSec@polito.it**

Direzione Ce.S.I.T.: **Piero BOZZA**

(Prof. Marco MEZZALAMA)