N. 27 Reg. Circolari
2009

09200900705
PROCURA GENERALE REPUBBLICA CAGLIARI
N. 2509 E. 29 APR. 2009
UOR INFORMATICA CC RUO SABA
Funzione 4 Macroattività 1 Attività
Fascicolo INFORMATICA Sottofascicoli GEST. SIST. INF.

Ministero della Giustizia

Dipartimento dell'organizzazione giudiziaria del personale e dei servizi

Direzione generale per i sistemi informativi automatizzati

m_dg.DOG07.29/04/2009.0013109.U

Al Sig. Primo Presidente
Al Sig. Procuratore Generale presso la
CORTE DI CASSAZIONE - ROMA
Al Sig. Presidente
TRIBUNALE SUPERIORE DELLE ACQUE PUBBLICHE – ROMA
Ai Sigg.ri Presidenti
Ai Sigg.ri Procuratori Generali presso le
CORTI DI APPELLO
LORO SEDI
Al Sig. Procuratore Nazionale Antimafia - ROMA

***Oggetto**: sicurezza delle postazioni di lavoro.*

Recentemente, e sempre più spesso, numerose postazioni di lavoro sono oggetto di attacchi da parte di virus informatici (da ultimo Confiker) che, introdotti mediante improprie ed imprudenti condotte, determinano gravissimo pericolo alla funzionalità dell'intero sistema informatico.

Una efficace prevenzione un valido contrasto di tali pericoli sono possibili solo a condizione che si proceda:

1. *al costante aggiornamento del sistema operativo (generalmente MS Windows)*
2. *al costante aggiornamento dell'antivirus (prevalentemente MacAfee)*
3. *all'installazione dei soli programmi autorizzati.*

Nell'attuale contesto le attività di cui sopra sono attribuite alla responsabilità del dipendente, il quale deve agire manualmente sulla propria postazione di lavoro per effettuare gli aggiornamenti necessari. Si è riscontrato, in effetti, che l'aggiornamento dei sistemi e dell'antivirus non viene effettuato con la dovuta regolarità, mentre non vi è alcun controllo sulla installazione di programmi disponibili su internet o introdotti in altro modo.

Le conseguenze di tale situazione sono gravissime: diffusione di virus che si estendono da una postazione all'altra, blocco progressivo di numerosi pc che si infettano tramite la rete, con continua epidemia dei sistemi che, seppur bonificati, continuano ad infettarsi a causa del permanere delle condizioni di rischio sopra indicate.

È ineludibile rimuovere le cause di tali pericoli, predisponendo un sistema di sicurezza in grado di:

a) *autenticare in maniera sicura gli utenti e le risorse in modo da evitare accessi illeciti;*
b) *limitare la possibilità per l'utente di installare, senza alcun controllo, programmi pericolosi;*

V. In Cagliari, addì 04 MAG. 2009

Il Dirigente Amm.vo
Franca Arru

V. In Cagliari, addì 29 APR. 2009

Il Procuratore Generale
Ettore Angioni

c) censire i pc in rete;
d) monitorarne il grado di funzionalità ed il livello di aggiornamento,
e) procedere alla effettuazione di aggiornamenti automatici del sistema operativo e dell'antivirus.

Gli obiettivi sopra indicati possono essere raggiunti unicamente attraverso:

- il dispiegamento della infrastruttura di autenticazione denominata ADN (Active Directory Nazionale), realizzata da questa direzione secondo le indicazioni del CNIPA,
- il dispiegamento di strumenti di monitoraggio e gestione remota delle postazioni di lavoro, certificati dal CNIPA nell'ambito del SPC (Sistema Pubblico di Connettività).

Le infrastrutture di cui sopra sono poste sotto il diretto controllo di questo Responsabile per i Sistemi Informativi Automatizzati che si avvale del personale tecnico dell'Amministrazione, sia a livello centrale (DGSIA e Centro Gestione Firewall di Napoli), sia a livello periferico (i CISIA e, a livello di ufficio, gli amministratori di sistema). La presenza di personale tecnico esterno, appositamente qualificato e controllato nell'ambito del SPC (Sistema Pubblico di Connettività), consente, inoltre, un costante presidio delle postazioni di lavoro.

Gli strumenti di monitoraggio e gestione remota delle postazioni di lavoro, che –come si è detto- sono stati certificati dal CNIPA, sono caratterizzati dalla assoluta trasparenza delle attività svolte dall'operatore il quale, previa autorizzazione dell'utente che effettua la chiamata, interviene sul pc per rimuovere direttamente il malfunzionamento o per fare intervenire il presidio territoriale. È importante sottolineare che tale attività, di volta in volta autorizzata dall'utente, viene comunque puntualmente e dettagliatamente registrata, con conservazione dei log di accesso e delle operazioni effettuate a disposizione dell'utente medesimo, oltre che del capo dell'ufficio e del personale tecnico dell'amministrazione. Inoltre i curricula vitae e le certificazioni di moralità e buona condotta degli operatori sono state puntualmente verificate da questa direzione; le stesse sono comunque a disposizione degli uffici giudiziari.

Questo Responsabile, nel restare a disposizione delle Autorità in indirizzo per ogni opportuno chiarimento, procederà al dispiegamento dei sistemi di cui sopra nell'ambito dei compiti attribuitigli.

Si pregano i vertici dei distretti di voler informare gli uffici giudiziari di quanto sopra.

Il Direttore Generale
Stefano Aprile