# INDICE



# INDICE DELLE FIGURE

## *INTRODUZIONE*

Questo vuole essere un breve esempio di come potrebbero essere scritte le regole aziendali per l'utilizzo delle attrezzature informatiche presso la ditta ***PINCOPALLINO***.

Si compone essenzialmente di due parti distinte; un elenco di norme comportamentali da distribuire a tutti i dipendenti e da rendere pubblico sull'eventuale Intranet Aziendale, se presente, ed un esempio di modulo da fare firmare per accettazione per abilitare l'utente all'utilizzo della posta elettronica e di Internet.

Premesso ciò ipotizzo per la ditta PINCOPALLINO l'esistenza di una rete locale, Intranet, dotata dei classici servizi di File e Print Server, di posta elettronica Interna, di Web server interno per l'Intranet, di accesso esterno ad Internet per il Web e di posta elettronica esterna.

Suppongo che la rete sia gestita da server Novell, che la posta elettronica sia gestita da Novell Groupwise e che l'accesso ad Internet sia controllato da Novell Border Manager.

## BREVE DESCRIZIONE DELLA RETE AZIENDALE.

Tutti i calcolatori della Società ***PINCOPALLINO*** sono collegati tra loro mediante una rete locale (Intranet) basata su Ethernet con protocollo TCP/IP.

Il cablaggio della rete è di tipo strutturato. Tutti i cavi inerenti la trasmissione Dati e la fonia sono raccolti in un armadio detto di permutazioni nel quale mediante opportuni cavetti, detti patch cord, vengono collegate le singole torrette alle rispettive utenze. Si prega quindi gli utenti a prestare la massima attenzione a non collegare erroneamente telefoni o calcolatori alle torrette. La connessione di nuovi apparati o la rimozione di apparati esistenti, siano essi telefoni, calcolatori o stampanti, deve sempre essere effettuata a cura del personale addetto.

Gli utenti non sono autorizzati per nessun motivo a modificare i cablaggi negli armadi; il collegamento errato di apparati può danneggiare le schede degli Switch o le schede del Centralino Telefonico.

I servizi di rete sono forniti da sistemi e server dedicati:

- Sistema Operativo LINUX - servizi Intranet di area, servizio Internet
- Sistema Operativo NOVELL - servizi di condivisione file, programmi, stampa, posta elettronica, accesso Internet e DHCP

## BREVI NOTE SUGLI INDIRIZZI IP E DHCP.

In una rete basata su TCP/IP ogni apparato di rete è caratterizzato dall'avere un suo indirizzo univoco, indirizzo IP, ed una maschera di sottorete. Questi indirizzi sono espressi nella forma xxx.xxx.xxx.xxx dove x assume valori da 0 a 254.

L'indirizzo è diviso in modo logico in due parti; un indirizzo di rete ed un indirizzo di macchina all'interno della rete.

**Affinché tutto funzioni è indispensabile che ogni macchina abbia un suo indirizzo IP univoco; all'interno della stessa rete non possono esistere due macchine con lo stesso indirizzo IP. Se per errore due macchine presentano lo stesso indirizzo le due interfacce di rete si bloccano**.

Questo può essere particolarmente dannoso qualora si tratti di una stazione di lavoro in conflitto con l'indirizzo di un server o di uno Switch della rete, perché in questo caso in pratica viene bloccato tutto il funzionamento. L'unico rimedio è quello di riavviare le macchine che hanno causato il conflitto di indirizzi con conseguente perdita di tempo da parte di tutti gli utenti.

E' quindi essenziale prestare la massima attenzione a non usare indirizzi IP casuali per configurare PC o altre attrezzature.

A seconda del numero di bit riservati all'indirizzo di rete e di quelli riservati all'indirizzo di macchina le reti si dividono in Classe A, B e C. Per ogni classe ci sono degli indirizzi IP liberi da usarsi per le reti private (Intranet) non registrate. A seconda del tipo di rete troviamo i seguenti indirizzi per le reti private non registrate:

| | |
|---|---|
| Classe A | da 10.0.0.0 a 10.255.225.255 con subnet 255.0.0.0 (una rete di classe A) |
| Classe B | da 172.16.0.0 a 172.31.255.255 con subnet 255.255.0.0 (16 reti di classe B) |
| Classe C | da 192.168.0.0 a 192.168.255.255 con subnet 255.255.255.0 (256 reti di classe C) |

La regola fondamentale delle reti IP è che gli indirizzi sono gerarchici: possono comunicare tra loro tutte e solo le macchine appartenenti alla stessa rete. Un esempio con una rete di classe C:

| NOME PC | Indirizzo IP | Subnet Mask |
|---|---|---|
| **PC-A** | **10.10.1.1** | **255.255.255.0** |
| **PC-B** | **10.10.1.2** | **255.255.255.0** |
| PC-C | 10.10.2.3 | 255.255.255.0 |

Nell'esempio indicato, i due PC A e B appartengono alla stessa rete e quindi comunicano tra loro, mente il PC C appartiene ad un'altra rete e quindi non comunica con gli altri due. Per collegare le due reti occorre un dispositivo denominato router, ovvero un'apparato in grado di instradare i pacchetti tra due reti diverse.

La rete aziendale della società ***PINCOPALLINO*** utilizza indirizzi di classe A con indirizzo di rete 10, ovvero indirizzi della famiglia 10.xxx.xxx.xxx con subnet mask 255.0.0.0

Ad oggi esistono alcune stazioni di lavoro configurate con IP statici, secondo la vecchia configurazione di rete. Le nuove macchine invece vengono installate tutte con indirizzi dinamici assegnati da un server DHCP per minimizzare il rischio di indirizzi duplicati.

Gli indirizzi di rete aziendale sono suddivisi in modo logico, in base alla tipologia delle macchine e dei servizi, come indicato nella seguente tabella:

| Range IP | Descrizione |
|---|---|
| 10.1.1.xxx | Riservata ai Server |
| 10.1.2.xxx | Riservata al management di Switch ed Hub |
| 10.1.3.xxx | Riservata alle stampanti |
| 10.10.1.xxx – 10.10.254.254 | Riservata al DHCP server per assegnare indirizzi dinamici ai PC |
| 10.20.1.xxx – 10.20.254.254 | Riservata per particolari esigenze di IP Statici |

La suddivisione logica degli indirizzi può subire modifiche nel tempo in funzione delle mutate esigenze di rete, e quando avviene una variazione viene data comunicazione alle aree interessate.
L'accesso alla rete può avvenire solo ed esclusivamente utilizzando i cablaggi predisposti dall'azienda
**Qualsiasi altro sistema per accedere alla rete, diverso da quello definito dall'azienda, è espressamente vietato salvo particolari autorizzazioni. Sono quindi da ritenersi vietati cavi o cablaggi non certificati, hub/switch/router direttamente connessi alla rete, o qualsiasi altro apparato atto a realizzare una connessione alla rete aziendale.**

## CONFIGURAZIONE PC AZIENDALI.

La società ***PINCOPALLINO*** mette a disposizione degli utenti gli strumenti informatici necessari alle loro attività. La procedura per ottenere tali strumenti prevede che il responsabile di area quando ha necessità di creare una nuova postazione o ha un fabbisogno informatico (aggiunta di una stampante, installazione software, abilitazione alla rete aziendale/Intranet, installazione multi-boot, aggiunta seriali ecc..), deve inoltrare richiesta al CED che provvederà ad evaderla al più presto compatibilmente con le eventuali autorizzazioni da richiedere.

**Si fa presente che il software è protetto dalle leggi sul diritto d'autore pertanto l'installazione di software non autorizzato è illegale, soprattutto nel caso di software di cui non si possiedono le regolari licenze di uso. L'utente è responsabile del PC che ha in dotazione, ed è quindi ritenuto direttamente responsabile nel caso di installazione non autorizzata di software.**

**Nel caso di PC usati da più utenti, l'incarico di verificare la regolarità del software installato è assegnato al responsabile di reparto a cui sono stati assegnati.**

I PC aziendali sono suddivisi in tre tipologie :

- PC connessi alla rete aziendale ad uso ufficio
- PC connessi alla rete aziendale ad uso CAD
- PC non connessi alla rete aziendali e PC portatili

La configurazione è diversa in base alla tipologia come di seguito indicato.

## PC CONNESSI ALLA RETE AZIENDALE AD USO UFFICIO

PC dotati di processore classe Celeron/Pentium III con sistema operativo Windows 2000 e monitor da 15" a 17" in funzione dell'utilizzo. Sono di base installati i programmi :

- client Novell per l'accesso ai dati/programmi della rete aziendale
- programmi per office automation Microsoft OFFICE 2000 SR-1
- programma di compressione/decompressione files PowerArchiver 2000
- programma antivirus Norton
- browser Microsoft Internet Explorer 6.0
- posta elettronica Novell Groupwise 5.5
- visualizzatore files in formato PDF Adobe Acrobat Reader

L'installazione e manutenzione degli applicativi indicati è responsabilità del personale del CED.

## PC CONNESSI ALLA RETE AZIENDALE AD USO CAD

PC dotati di processore classe Pentium IV con sistema operativo Windows 2000 e monitor 21". Sono di base installati i programmi :

- client Novell per l'accesso ai dati/programmi della rete aziendale
- programmi per office automation Microsoft OFFICE 2000 SR-1
- programma di compressione/decompressione files PowerArchiver 2000
- programma antivirus Norton

- browser Microsoft Internet Explorer 6.0
- posta elettronica Novell Groupwise 5.5
- visualizzatore files in formato PDF Adobe Acrobat Reader
- AutoCad 13 Compreso di librerie

L'installazione e manutenzione degli applicativi indicati è responsabilità del personale del CED.

### PC NON CONNESSI ALLA RETE AZIENDALE E PC PORTATILI

PC dotati di processore classe Celeron con sistema operativo Windows 98. Sono di base installati i programmi :

- programmi per office automation Microsoft OFFICE 2000 SR-1 (dove necessario)
- programma di compressione/decompressione files PowerArchiver 2000
- programma antivirus Norton
- visualizzatore files in formato PDF Adobe Acrobat Reader

L'installazione e manutenzione degli applicativi indicati è responsabilità del personale del CED.

## NORME DI UTILIZZO DELLA INTRANET AZIENDALE

Le regole informatiche definite dall'azienda sono disponibili sul sito Intranet della Società ***PINCOPALLINO*** alla sezione "regole informatiche".
La conoscenza di tali regole è di fondamentale importanza, con particolare riferimento alla sicurezza dei dati e al corretto utilizzo degli strumenti informatici, pertanto segue un riassunto di tali regole che ciascuno deve seguire:

- l'accesso all'elaboratore, sia esso in rete o "stand alone", è sempre protetto da una o più password. La password assegnata non deve essere divulgata e deve essere custodita dall'assegnatario con la massima diligenza
- è tassativamente proibito installare programmi provenienti dall'esterno se non con autorizzazione esplicita
- il personal computer deve essere spento ogni sera prima di lasciare gli uffici, salvo diverse disposizioni o in caso di particolare necessità. Durante la pausa pranzo deve essere effettuato il salvataggio e la chiusura di tutti i files aperti, per non ostacolare eventuali attività di amministrazione di sistema, e impostare il blocco dell'elaboratore tramite la combinazione dei tasti CTRL+ALT+CANC e scegliendo il pulsante Lock Workstation
- gli utenti devono effettuare le stampe dei dati solo se strettamente necessarie e ritirarle immediatamente dai vassoi delle stampanti comuni
- la casella personale di posta elettronica interna deve essere mantenuta in ordine, cancellando i documenti inutili, specialmente se contengono allegati ingombranti. Deve essere compilato sempre il soggetto mittente e non devono essere inviati messaggi completamente estranei al rapporto di lavoro
- agli utenti assegnatari delle caselle di posta elettronica Internet è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list salvo diversa ed esplicita autorizzazione
- agli utenti che hanno accesso ad Internet non è consentita la consultazione di caselle di posta elettronica personali in nessuna forma compreso l'accesso via browser alle webmail
- gli utenti che hanno accesso ad Internet debbono evitare lo scaricamento di programmi software, anche gratuiti, se non per esigenze strettamente professionali e fatti comunque salvi i casi di esplicita autorizzazione
- agli utenti che hanno accesso ad Internet è tassativamente proibito effettuare ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure per gli acquisti
- agli utenti che hanno accesso ad Internet è vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e la registrazione in guest books anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti all'attività professionale.

## NORME DI SICUREZZA PER L'USO DEI PERSONAL COMPUTER ED ATTREZZATURE ELETTRONICHE

Personal Computer, workstation, server, terminali, monitor e stampanti sono apparecchiature elettriche, ed il loro utilizzo richiede un minimo di attenzione per evitare spiacevoli sorprese.

Pertanto :

- non accendete il PC o il terminale quando sono aperti per evitare folgorazioni
- non maneggiate il PC o il terminale con le mani bagnate o umide, soprattutto se dovete accenderli o spegnerli, per evitare folgorazioni
- non pulite il monitor con liquidi detergenti, specie se infiammabili, quando è acceso o semplicemente collegato alla presa di corrente
- ricordatevi alla sera, od ogni qual volta dovete abbandonare la vostra postazione per un tempo prolungato, di spegnere il PC o la workstation per minimizzare i rischi di incendio
- evitate di chiudere le feritoie di areazione del PC, workstation, terminale e soprattutto del monitor (ad esempio appoggiando carta sopra al monitor) per evitare possibili surriscaldamenti e principi di incendio
- cercate di mantenere una posizione corretta, non tenete il monitor troppo luminoso o troppo vicino al viso per prevenire danni alla vista.

## ISTRUZIONI OPERATIVE

L'utilizzo delle risorse informatiche, telematiche e del patrimonio informativo della nostra Società deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che il dipendente è sempre tenuto ad adottare nell'ambito del rapporto di lavoro.

Pertanto ogni utilizzo delle apparecchiature, degli elaboratori, delle reti e dei dati diversi dalle finalità strettamente professionali è espressamente vietato.

Tuttavia poiché anche nella normale attività lavorativa alcuni comportamenti possono mettere a rischio la sicurezza e l'immagine aziendali, di seguito vengono richiamate semplici regole comportamentali finalizzate non tanto a censurare comportamenti consapevolmente scorretti già di per se proibiti, ma soprattutto per evitare condotte che inconsapevolmente possano causare rischi alla sicurezza del trattamento dei dati.

La Società ***PINCOPALLINO*** predispone regolari momenti formativi ed informativi per garantire a tutti gli incaricati il massimo aggiornamento in merito ai rischi, alle procedure operative, alla prevenzione dei danni e, più in generale, alle problematiche relative alla sicurezza in materia di trattamento dei dati.

## UTILIZZO DELL'ELABORATORE E DELLA RETE INTERNA (INTRANET)

L'accesso all'elaboratore, sia esso in rete o "stand alone", è sempre protetto da una o più password. La password assegnata non deve essere divulgata e deve essere custodita dall'assegnatario con la massima diligenza. Ogni 6 mesi il sistema obbliga gli utenti al cambio password, non si possono utilizzare le vecchie password. Per chiarimenti in merito alle modalità di cambio password si consulti la sezione Cambio Password sull'intranet aziendale Possono essere introdotte limitazioni all'accesso agli archivi laddove il Responsabile del loro trattamento lo ritenga opportuno.
È tassativamente proibito installare programmi provenienti dall'esterno se non con autorizzazione esplicita, in quanto l'utilizzo di software non regolarmente acquistato dalla Società può configurare un reato nonché in considerazione del grave pericolo di contrarre virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Su queste unità vengono svolte regolari attività di controllo, amministrazione e backup. Periodicamente si procede alla pulizia degli archivi, con cancellazione o spostamento su unità locali dei files obsoleti o inutili. Viene prestata particolare attenzione alla duplicazione dei dati.

ATTENZIONE: il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici, salvo diverse disposizioni o in caso di particolare necessità. Durante la pausa pranzo deve essere effettuato il salvataggio e la chiusura di tutti i files aperti, per non ostacolare eventuali attività di amministrazione di sistema, e impostare il blocco dell'elaboratore tramite la combinazione dei tasti CTRL+ALT+CANC e scegliendo il pulsante Lock Workstation.

Tutti i supporti magnetici riutilizzabili (dischetti, cassette, cartucce) contenenti dati personali devono essere trattati con particolare cautela. Il supporto, al termine dell'utilizzo, deve essere riformattato a garanzia che il suo riutilizzo sia assolutamente sicuro.

ATTENZIONE: gli utenti devono effettuare le stampe dei dati solo se strettamente necessarie e ritirarle immediatamente dai vassoi delle stampanti comuni.

I fornitori esterni, addetti alla manutenzione di hardware, software e reti, operano in conformità alle presenti istruzioni, sotto la sorveglianza dei Responsabili del trattamento.

## PC E ATTREZZATURE PORTATILI.

La Società ***PINCOPALLINO*** mette a disposizione dei dipendenti alcuni PC portatili il cui utilizzo deve essere autorizzato. Le regole di utilizzo di queste apparecchiature sono le medesime indicate per i PC connessi alla rete, con una particolare attenzione alla rimozione di eventuali files elaborati sullo stesso prima della riconsegna.

L'utilizzo di attrezzature personali (PC portatili, unità di backup, modem, masterizzatori ecc...) è tassativamente proibito salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali regole informatiche.

## *La Posta Elettronica*

La posta elettronica interna funziona in architettura client/server. Sulle singole stazioni di lavoro è installato il client GroupWise che si interfaccia con il server di posta.

Rispetto ai tradizionali programmi di gestione della posta elettronica tipo Outlook express, Eudora ecc.. l'architettura di GroupWise prevede la gestione delle caselle postali degli utenti direttamente sul server. I messaggi di posta elettronica e le rubriche sono quindi memorizzate in un database sui dischi del server e questo garantisce la possibilità di includere anche gli archivi della posta elettronica nelle usuali operazioni di salvataggio.

Il sistema di messaggistica prevede due diversi livelli di abilitazione all'invio di posta elettronica:

- solo posta elettronica interna
- posta elettronica interna e accesso alla posta elettronica esterna

Ai singoli utenti viene concessa l'abilitazione della posta elettronica interna e a seconda delle loro necessità l'abilitazione alla posta elettronica esterna.

Per gli utenti abilitati all'invio della posta elettronica esterna è prevista una massima dimensione dei messaggi inviabili in base alle specifiche necessità dei singoli.

La scelta aziendale è quella di utilizzare GroupWise per la gestione della messaggistica. Non devono assolutamente essere usati altri metodi di gestione della posta, perché in tal caso vengono meno alcune funzioni ritenute indispensabili per un corretto utilizzo della posta interna. Tra queste funzioni è ritenuta fondamentale la possibilità di avere il riscontro sulle aperture dei messaggi da parte dei destinatari. L'utilizzo di altri metodi di accesso alla casella postale non offre questa possibilità, quindi accade che il destinatario abbia ricevuto e letto regolarmente il messaggio senza che il mittente sia in grado di avere una segnalazione dell'avvenuta apertura dello stesso.

### Posta Elettronica Interna.

La casella personale di posta elettronica interna deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti al fine di non sprecare spazio sui dischi del Server di Posta.

Deve essere compilato sempre il soggetto mittente e non devono essere inviati messaggi completamente estranei al rapporto di lavoro.

Viene utilizzata automaticamente dal sistema la ricevuta di ritorno per avere la conferma della avvenuta lettura del messaggio da parte del destinatario.

### Posta Elettronica Esterna.

L'utilizzo degli strumenti di comunicazione telematici deve necessariamente fare riferimento alle procedure in essere per quanto attiene alla verifica e circolazione delle comunicazioni prodotte o ricevute.

In generale ogni comunicazione inviata o ricevuta che abbia contenuti significativi o contenga impegni contrattuali o precontrattuali per la Società ***PINCOPALLINO*** deve essere visionata od autorizzata dalla Direzione e comunque si fa riferimento alle procedure in essere per la corrispondenza ordinaria.

Le persone assegnatarie delle caselle di posta elettronica Internet sono responsabili del corretto utilizzo delle stesse.

Pertanto è fatto divieto di utilizzare le caselle di posta elettronica per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list salvo diversa ed esplicita autorizzazione da parte della Direzione.

Attraverso la rete interna della Società ***PINCOPALLINO*** non è consentita la consultazione di caselle di posta elettronica personali in nessuna forma compreso l'accesso via browser alle varie WebMail.

La posta elettronica inviata all'esterno o ricevuta dall'esterno mediante GroupWise viene copiata in un archivio delle e-mail aziendali, come indicato nella lettera riportata in seguito che viene fatta firmare a tutti gli utenti abilitati all'utilizzo della posta elettronica esterna.

L'azienda mantiene un archivio della posta elettronica aziendale esterna in cui sono memorizzati tutti i messaggi inviati dalla Società PINCOPALLINO verso il mondo esterno e di tutti i messaggi inviati dal mondo esterno verso alla Società PINCOPALLINO

### *COPIA DEL MESSAGGIO DI POSTA CHE VIENE INVIATO AI NUOVI UTENTI IN SEGUITO ALL'ABILITAZIONE DEL SERVIZIO DI MAIL CON ACCESSO ESTERNO.*

Egregio signor Mario Rossi,

a partire dalla data odierna la sua utenza è abilitata alla trasmissione e ricezione diretta dei messaggi e-mail tramite INTERNET.

Le modalità di utilizzo del servizio sono:

- l'indirizzo per ricevere email è MARIO.ROSSI@dominio.della.società.
- le email in entrata non hanno alcun limite in termini di dimensioni.
- le email in uscita compresi gli allegati sono limitate alla dimensione 1,5 MByte. A seconda dei casi sono ammesse deroghe per email di dimensione superiori
- il servizio è attivo sempre, eccetto durante le operazioni di manutenzione del sistema che verranno tempestivamente comunicate

*Si rammenta che la posta elettronica trasmessa e/o ricevuta tramite Internet è considerata, per motivi organizzativi, una componente del circuito di comunicazione aziendale e quindi può essere trasferita in copia ad uno o più archivi e/o utilizzata da altri Enti o Reparti aziendali.*

Pertanto l'abilitazione al servizio è condizionata alla firma del consenso per il trattamento dei dati personali, come indicato nella Legge 31 dicembre 1996 n.675, che viene richiesta dall'Ufficio Personale.

## NOTE SULLA PRIVACY DELLA POSTA ELETTRONICA

Il Garante per la privacy assimila la posta elettronica a quella ordinaria quindi:

- la corrispondenza elettronica ha la stessa tutela di quella "ordinaria"
- le caselle di posta elettronica, le mailing list, i newsgroup "chiusi" sono equiparati ai "normali" recapiti per la "normale" corrispondenza su carta. Conseguenza: i messaggi via Internet sono soggetti alla stessa tutela di quelli che ci vengono portati a casa dal postino; in entrambi i casi, chi li intercetta compie il reato penale di violazione di corrispondenza.
- E-mail, liste, newsgroup non possono essere violati

sono quindi equiparati alla normale posta elettronica. Nel caso dei newsgroup ovviamente si deve intendere solo i newsgroup chiusi ovvero quelli che richiedono una password di accesso. I newsgroup pubblici ovviamente sono esclusi da queste valutazioni.
Il principio vale anche per gli account aziendali ma solo "fino a prova contraria"

Chi utilizza indirizzi e-mail presso i server dell'azienda, o dell'istituzione, in cui lavora, può rivendicare il diritto alla riservatezza dei contenuti spediti o ricevuti "fino a prova contraria". Cioè fino a quando l'ente in questione non chiarisce formalmente, mettendolo nero su bianco, che tutti i testi in entrata o in uscita da qualsiasi account "interno" possono essere resi pubblici in qualsiasi momento.

Il Garante prevede che la posta elettronica personale sia segreta, e questo vale per le caselle personali che un'utente registra sui server degli Internet Service Provider. Nel caso degli account aziendali vige la stessa regola salvo prova contraria ovvero se l'azienda non segnala esplicitamente il fatto di archiviare e/o gestire in qualche modo la posta degli utenti questa deve essere considerata segreta.

## RICHIESTA DI PARERE ALL'AUTORITY PER LA RISERVATEZZA DEI DATI PERSONALI

Riportiamo la richiesta di parere all'Autorità che tutela la riservatezza dei dati personali, presieduta da Stefano Rodotà.

Lunedì, 12 luglio 1999

1) La posta elettronica come quella ordinaria. Il concetto era stato già espresso dall'Autorità, ma mai in forma così chiara ed organica. Intercettare una mail è dunque reato penale, quello di violazione di corrispondenza, come già stabilito dalla legge.
2) Mailing list e newsgroup. Il Garante equipara entrambi gli strumenti alla posta elettronica "singola", facendo dunque valere la stessa, completa tutela della riservatezza. Ad una condizione: i diritti totali alla privacy valgono solo per i newsgroup "chiusi", cioè quelli per il cui accesso è necessario digitare una parola chiave.
3) La posta elettronica aziendale. Il tema non è direttamente affrontato nel parere, ma in realtà la pronuncia dell'Autorità contiene indicazioni forti anche su questo punto, molto dibattuto nel nostro come in altri paesi (gli Usa in testa). In sostanza, il Garante non dice che l'account del singolo dipendente presso la propria azienda o istituzione vada considerato come corrispondenza personale, privata.

Il discorso è più complesso: secondo l'ufficio presieduto da Rodotà, infatti, il dovere dell'azienda è solo quello della chiarezza. In altri termini, fino a quando una società non comunica ufficialmente, e senza possibilità di equivoci, che tutti i messaggi inviati tramite l'indirizzo aziendale di ciascuno possono essere visibili da tutti e in qualsiasi momento, allora vuol dire che ciascun utente ha diritto alla più assoluta tutela della privacy. Nulla impedisce, però, alla società, di esplicitare questo vincolo: solo nel momento che questa "limitazione" nell'utilizzo viene chiarita, i diritti alla riservatezza decadono.

Per avere ulteriori chiarimenti su questo punto così delicato, ci si può riferire alle pagine internet del Garante della Privacy.

Stabilendo con certezza, attraverso regole comunicate ai dipendenti senza possibilità di equivoci, se si dà loro - o meno - la libertà di utilizzare l'indirizzo dell'ufficio in maniera riservata, oppure no.

Entrambe le possibilità sono legittime: ma se la società o l'ente non spiega qual è la regola, si intende che il lavoratore ha tutto il diritto a vedere tutelata la privacy". Il problema è solo chiarire se l'account va utilizzato per fini personali o esclusivamente professionali, oppure c'è una questione di riservatezza anche sulle informazioni di carattere professionale?

"La tutela dei dati vale anche sul fronte professionale. Se l'azienda vuole poter accedere alle informazioni di lavoro diffuse attraverso le mail dei suoi dipendenti, allora deve stabilire una volta per tutte la regola che qualsiasi messaggio può, in qualsiasi momento, essere reso pubblico. Se questa regola non viene fissata, allora la riservatezza per il dipendente è garantita. E quindi vale anche per i dati raccolti per motivi professionali".

## NAVIGAZIONE INTERNET

L'accesso ad Internet attraverso la rete aziendale è regolato da un proxy server Novell Border Manager che consente il traffico HTTP solo verso l'esterno ed il traffico FTP solo in ricezione. Attualmente non è quindi possibile inviare dati all'esterno mediante il protocollo FTP per motivi di sicurezza aziendale.

***L'utilizzo di metodi alternativi per accedere ad Internet e' tassativamente vietato per problemi di sicurezza.*** Collegandosi ad Internet tramite un modem in un PC connesso in rete aziendale, si pone a rischio integrità tutta la rete durante il tempo della connessione. Un malintenzionato può infatti introdursi nel PC connesso ad Internet mediante modem.

L'utilizzo di proxy server installati localmente per condividere con altri utenti l'accesso aziendale ad Internet e' assolutamente vietato. Oltre a causare un rallentamento del PC stesso a causa della gestione dell'elevato numero di files in cache, risulta che tutte le connessioni ad Internet effettuate dagli utenti del proxy server locale sono a carico dell'unico utente autenticato a Border Manager.

Si richiama l'attenzione degli utenti sul fatto che l'utilizzo dei degli strumenti per la navigazione su Internet è sottoposto alle seguenti verifiche e limitazioni sistematiche :

- è limitato l'accesso a siti non strettamente legati all'attività propria della Società (quali a titolo di esempio siti di società sportive, riviste sportive ...)
- è bloccato l'accesso ai siti che consentono di gestire le caselle email personali via web
- è bloccato l'accesso ai newsgroup
- l'attività in Internet viene tracciata da Border Manager mantenendo un log delle connessioni, in cui si evidenziano IP della macchia, indirizzo http richiesto data e ora della connessione. Tale log viene utilizzato esclusivamente per motivi di sicurezza. Non esistono altri fini in questa attività di controllo.

Dall'interno della rete aziendale, quindi: è da evitare lo scaricamento di programmi software, anche gratuiti, se non per esigenze strettamente professionali e fatti comunque salvi i casi di esplicita autorizzazione è tassativamente proibita l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dalla Direzione e con il rispetto delle normali procedure per gli acquisti è vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e la registrazione in guest books anche utilizzando pseudonimi (o nicknames) e, più in generale, qualunque utilizzo di servizi Internet, attuali o futuri, non strettamente inerenti all'attività professionale.

## BREVI NOTE SULLA SICUREZZA

### ACCOUNT UTENTI

L'accesso ai servizi aziendali prevede una gestione degli utenti che varia in funzione del servizio che si intende utilizzare. Per tutti i servizi offerti dalla rete di PC (file server, print server, posta elettronica, accesso Internet) la gestione degli utenti (account) è centralizzata tramite il servizio di autenticazione NOVELL NDS. In questo modo è possibile gestire gli account in modo univoco per tutti i server di rete in ambiente Novell Netware mediante Novell NDS.

Gli account con le relative autorizzazioni vengono creati dall'amministratore di rete che provvede a creare l'utente, definire la sua login al sistema (nome dell'utente) ed assegnargli una ***PASSWORD PROVVISORIA*** che viene comunicata all'utente per effettuare la prima login al sistema (valida per 6 login iniziali). E' quindi lasciato all'utente il compito di scegliersi la propria ***PASSWORD PERSONALE che deve essere mantenuta segreta***. L'amministratore di sistema non ha modo di leggere le password impostate dai singoli utenti ma può, solo in caso di necessità, revocare i diritti di accesso dell'utente o eventualmente azzerargli la PASSWORD reimpostando una nuova PASSWORD PROVVISORIA.
In nessun caso l'amministratore può ripristinare la password impostata dagli utenti, può solo azzerarla!.

### SCAMBIO AUGURI TRAMITE POSTA ELETTRONICA CON ALLEGATI

In occasione delle tradizionali festività è uso scambiare messaggi augurali mediante posta tradizionale o elettronica.

Sfortunatamente la posta tradizionale spesso arriva in ritardo ed ha costi superiori. Sempre più utenti decidono quindi di utilizzare la posta elettronica per lo scambio di auguri.

La posta elettronica giunge puntuale e costa quasi nulla, e assieme ad essa arrivano puntuali gli allegati carichi di "virus" o "sorprese nascoste".

Si raccomanda pertanto di prestare la massima attenzione ai messaggi ricevuti in questo periodo, ed in NESSUN CASO APRIRE ALLEGATI NEI FORMATI ESEGUIBILI ovvero programmi con estensione .exe .com .bat .pif).

Quindi se trovate ad esempio un allegato con i nomi auguri.EXE oppure auguri.COM oppure auguri.jpg.EXE NON DOVETE ASSOLUTAMENTE APRIRLO O ESEGUIRLO !!.

Anche un programma apparentemente innocuo che visualizza decorazioni natalizie sullo schermo o animazioni con personaggi natalizi ecc.. può nascondere dei comandi che a vostra insaputa danneggiano il PC o la rete ed i dati in essi contenuti.

Per qualsiasi ulteriore chiarimento rivolgersi al reparto Information System.

### RISCHIO VIRUS, CAVALLI DI TROIA, BACKDOOR ECC.

La rete aziendale è protetta dall'antivirus Norton. I programmi antivirus non possono comunque offrire una sicurezza totale nei confronti dei virus. Per chi non avesse le idee chiare sull'argomento, un virus altro non è che un programma scritto con intenzione di fare danni, ma è comunque un programma. A priori dire che un virus è diverso da un programma è impossibile, quindi gli antivirus devono ricorrere ad una analisi dei contenuti eseguendo una ricerca per testi all'interno dei singoli files, in cerca di elementi noti per quel determinato virus.
Si dice che gli antivirus devono essere periodicamente aggiornati, perché si deve aggiornare il dizionario delle definizioni dei virus. Esiste un certo periodo di tempo da quando un virus viene diffuso a quando vengono analizzati i primi danni del virus, con analisi del tipo di virus e conseguente aggiornamento del dizionario delle definizioni dei virus. Solo dopo qualche tempo quindi i programmi antivirus riusciranno ad intercettarlo correttamente.
Oltre ad un buon antivirus mantenuto aggiornato è quindi richiesta la massima attenzione quando vengono scaricati programmi o files in genere da Internet, e quando si ricevono allegati alla posta elettronica.
I primi virus erano semplici programmi eseguibili (files con estensione .EXE, .COM, .BAT, .PIF) e quindi era relativamente semplice cercare di neutralizzarli, il rischio virus esisteva solo con i files eseguibili ovvero i programmi. Non si correvano pericoli invece con i semplici files di dati. Con la progressiva diffusione di programmi tipo Microsoft Office, dotati di funzionalità di programmazione mediante il meccanismo delle Macro oppure con documenti in HTML o XML che possono contenere elementi attivi (Javascript ed ActiveX), il rischio virus si è spostato anche sui semplici files di dati. Oggi un normale documento Microsoft Word o un foglio di calcolo Microsoft Excel possono racchiudere pericolosissimi virus delle Macro. Microsoft Office prevede un meccanismo di protezione nei confronti delle macro non firmate che presenta ancora notevoli vulnerabilità.

## Danni da Virus

I danni causati dai Virus sono di vario genere, a partire dai virus che potremmo definire innocui che si limitano a consumare risorse del sistema (spazio su disco e/o ram) fino ai virus peggiori che arrivano a cancellare files, direttori ed a volte anche interi dischi fissi. Il pericolo di attacchi da virus non deve quindi essere mai sottovalutato.
La Legge in particolare prevede il Crimine Informatico qualora si diffondano volontariamente virus o qualora non si prendano le necessarie precauzioni per evitarne la diffusione.

## Cavalli di Troia

Nella generica categoria virus possiamo fare ricadere anche i programmi definiti Cavalli di Troia ovvero quei programmi che, con aria innocua, consentono di inserire programmi malefici che possono attivarsi improvvisamente a distanza di tempo e causare danni. Rispetto ai classici virus sono più difficili da identificare, anche perché la finestra temporale in cui non vengono riconosciuti dagli antivirus può essere abbastanza ampia. Diffondendo infatti un programma che diventerà attivo dopo parecchio tempo, si hanno buone speranze di distribuirlo in diversi PC prima che vengano segnalati danni e quindi possa essere bloccato dagli antivirus.

## Back Door

In questo caso le cose sono leggermente più complesse da spiegare. Caricando un generico programma che svolge regolarmente la sua funzione, ad esempio di invio della posta elettronica, questo programma potrebbe installare nel sistema delle porte di accesso nascoste che possono essere successivamente utilizzate da malintenzionati per accedere abusivamente al sistema. Queste porte non sono altro che passaggi in grado di aggirare le procedure di sicurezza.

Un sistema compromesso con delle Back Door a priori può funzionare normalmente ma da remoto resta controllabile. I vari attacchi su internet ai vari siti sono spesso effettuati con la collaborazione inconsapevole di molti sistemi violati precedentemente, che a comando eseguono determinate azioni ad esempio di disturbo, verso altri sistemi.

In questo caso si potrebbe dire che gli hacker siano interessati alla Cpu, ai dischi del sistema ed all'identità degli ingari utenti piuttosto che ai dati contenuti nel sistema.

Eventuali azioni di disturbo o attacchi a siti risulterebbero infatti effettuati dagli ignari utenti di quei sistemi lasciando i veri responsabili nell'ombra.

## I rischi del software in genere

Tutto quello che è stato detto in merito ai virus vale comunque anche per i normali programmi. Installare un generico programma di fonte sconosciuta, oltre ovviamente ad essere un illecito ai sensi della legge sulla tutela del software, può mettere a rischio la sicurezza della macchina o dell'intero sistema perché il programma può a sua volta contenere codice nascosto che compie a nostra insaputa anche altre azioni. Un programma di posta elettronica potrebbe per esempio svolgere regolarmente le sue funzioni di client di posta elettronica ed inviare periodicamente i files delle password ad un determinato sito di hacker il tutto in modo trasparente all'utente.

La migliore arma di difesa nei confronti di questi potenziali rischi risulta quindi essere la prudenza: non installare mai software di origini ignote e soprattutto evitare di installare del software solo per provarlo. L'installazione di programmi inutili oltre a mettere a rischio il sistema, causa sicuramente problemi di velocità del calcolatore su cui viene installato. In qualsiasi caso, per evitare che i rimedi siano peggiori del male, occorre ricordare di disinstallare eventuali programmi utilizzando esclusivamente gli appositi comandi di disinstallazione (dal pannello di controllo utilizzando installa/disinstalla applicazioni) o da menu dello stesso programma (utilizzando disinstalla). Non si devono mai disinstallare i programmi semplicemente cancellandoli dal disco fisso.

## Installazione software gratuito "adware"

Attraverso le riviste di informatica, tramite amici o tramite Internet sempre più spesso è possibile ottenere software gratuito "adware".

Cosa significa esattamente software "adware" ? Sono programmi di libera distribuzione che non hanno alcun costo per gli utenti finali. Chi sviluppa tali programmi si ripaga dei costi iniziali e di manutenzione inserendo avvisi pubblicitari ("advertisement", i famosi Banner) all'interno dell'applicazione. Se l'utente apprezza il programma, viene richiesto cortesemente di selezionare con il mouse ogni tanto la finestra che contiene le inserzioni ("banner"). L'operazione citata viene registrata nei siti remoti di poche compagnie (Cydoor, Radiate, Web3000), inserendo nel loro database anche le informazioni relative all'utente e al PC utilizzato.

## Cosa accade realmente quando vengono installati i programmi "adware" ?

All'atto dell'installazione del programma "adware", viene installato un altro programma nascosto che tenta di collegarsi al sito remoto con cadenza periodica di qualche secondo, in modo da trasmettere in tempo quasi reale le informazioni dell'utente e ricevere in tempo quasi reale nuovi "advertisement" da visualizzare nel "banner".

## Cosa accade sulla rete aziendale dopo l'installazione dei programmi "adware" ?

Sui PC e sulla rete aziendale si verificano le seguenti anomalie:

- il PC è costantemente impegnato a cercare di trasmettere e ricevere informazioni tramite Internet, e quindi la memoria e la capacità di elaborazione disponibile per i programmi aziendali diminuisce rendendo tutto più lento ed instabile (ATTENZIONE : questo vale anche se l'installazione è stata fatta da un altro utente e l'utente del PC in quel momento non ha l'accesso ad Internet oppure il PC è semplicemente acceso, in quanto il programma nascosto è sempre in funzione da quando si accende il PC)
- i server della rete vengono impegnati costantemente a cercare di comunicare con Internet e quindi il traffico di dati sulla rete aumenta inutilmente, rallentando tutti gli altri utenti di rete
- la sicurezza viene messa in pericolo perchè i dati trasmessi possono contenere informazioni anche sui dati presenti nel PC o sui dichi di rete, oppure la continua connessione può consentire l'accesso da remoto di malintenzionati

## E' possibile avere un elenco dei programmi "adware" ?

L'elenco è molto esteso, ma a titolo d'esempio possiamo citare i seguenti programmi "adware" tra i più noti:

- Babylon, traduttore e dizionario inglese/italiano
- Opera 5, browser per la navigazione su Internet (le versioni predenti erano a pagamento)
- Free Pics, visualizzatore di sfondi
- Html Tutor Pro, tool per insegnare come sviluppare pagine Web
- Free MP3, programma per ascoltare brani musicali MP3
- Contact Plus, programma per la gestione degli indirizzi
- Go!Zilla, programma per scaricare file da Internet
- Byo-Rhythms, visualizzatore di bio-ritmi
- Notepad+, sostituto del Notepad tradizionale di Windows
- CuteFtp, programma per gestire l'FTP con una simpatica interfaccia grafica

Non esiste quindi una categoria precisa di programmi "adware", ma qualsiasi programma può diventare "adware" a scelta del produttore (ad esempio Opera era a pagamento e per motivi commerciali è diventato "adware").

## Come comportarsi in azienda nei confronti del Software Adaware ?

Innanzitutto rispettare le regole aziendali, ovvero come indicato nelle Regole informatiche pubblicate sulla pagina Intranet e rispettare quanto segue:
"....È tassativamente proibito installare programmi provenienti dall'esterno se non con autorizzazione esplicita, in quanto l'utilizzo di software non regolarmente acquistato dalla Società può configurare un reato nonché in considerazione del grave pericolo di contrarre virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore..."

Inoltre, qualora siano stati installati programmi "adware", chiedere l'intervento immediato del personale addetto alla manutenzione dei PC affinché vengano rimossi nel modo appropriato.

ATTENZIONE : la semplice rimozione del programma "adware" non è sufficiente, in quanto il programma nascosto che comunica con i server remoti rimane installato e attivo, pertanto è necessario l'intervento di un addetto informatico per la rimozione effettiva dei programmi.

## *Norme di comportamento in presenza di virus hoax*

## Cosa sono i virus hoax ?

Spesso accade che in azienda vengano diffusi messaggi su virus informatici provenienti da varie fonti che spiegano l'approssimarsi di un virus tremendo e cose del genere. Purtroppo spesso propongono anche strani rimedi che non funzionano oppure fanno danni..

Abbiamo verificato che tali messaggi sono relativi ai cosiddetti "virus hoax", ovvero falsi avvisi su virus inesistenti che hanno effetti impossibili.

## Come riconoscere tali messaggi ?

Tipicamente i virus hoax sono messaggi e-mail che descrivono l'esistenza di un nuovo pericoloso virus non rilevabile dagli antivirus, a volte utilizzando termini di tipo tecnico. Il messaggio spesso prosegue avvisando di non leggere o aprire le mail che contengono un determinato oggetto, come il virus hoax Join the Crew, oppure avvisa che "..la CPU

del vostro computer eseguirà un loop binario infinito di n-esima complessità che può danneggiare fortemente il processore ...", come il virus hoax Good Times.

## Quali danni provocano i virus hoax ?

Gli unici veri danni arrecati all'azienda dalla diffusione di tali messaggi sono il tempo dedicato alla lettura ed invio di messaggi inutili da parte di tutti i destinatari e l'occupazione di spazio disco sui server di posta.

## Come comportarsi quando si riconosce un virus hoax ?

Non inoltrate messaggi relativi virus di qualsiasi tipo a nessuno tranne che al personale incaricato del CED. Non importa se tali messaggi provengono da produttori di anti-virus oppure se sono stati confermati da altre aziende o da vostri conoscenti.

Tutti i messaggi relativi ai virus debbono essere inviati esclusivamente al reparto Information System.

L'unica persona autorizzata a diffondere notizie relative ai virus è il responsabile del reparto Information System., qualsiasi altra fonte di informazioni deve essere ignorata.