
**Nuove sfide nella sicurezza:
perché worm e spam
sono una grave minaccia
per le imprese e i cittadini**

Lugano Communication Forum, 7 Aprile 2004

***Gigi Tagliapietra
Amministratore Delegato Siosistemi SpA
Comitato Direttivo CLUSIT***

I temi di oggi

- Il valore della sicurezza
- Le minacce
- Quale approccio
- La posta in gioco

I bisogni

La piramide di Maslow



La sicurezza è un bisogno

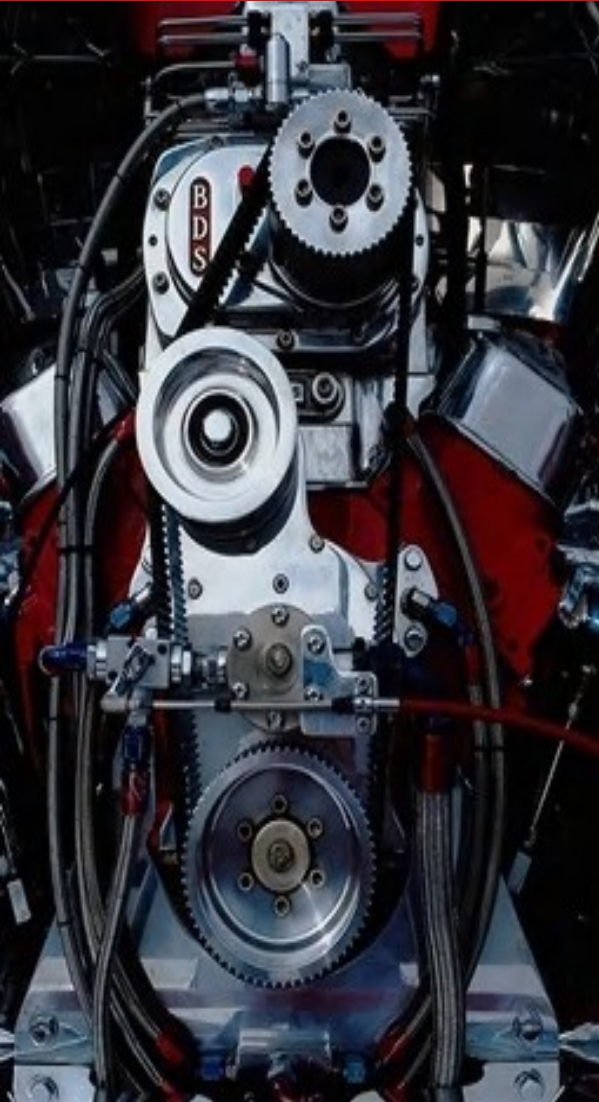


Il valore



- Sempre più le aziende vivono di informazioni
- Proteggere le informazioni vuol dire proteggere l'impresa
- Se l'informazione è seria va trattata seriamente
- La sicurezza della comunicazione digitale
 - ◆ il centro gravitazionale dell'intero sistema.
 - ◆ la condizione **affinché la comunicazione possa** non semplicemente agire, ma **essere**.

La tecnologia



- La tecnologia serve a ridurre i costi
- La tecnologia serve a fare meglio
- La tecnologia serve all'impossibile
- La tecnologia serve alla direzione

PRIMO PUNTO

Un ambiente
sicuro
sarà sempre più
un valore primario



Dati importanti



- **Uso di Internet**
 - 1999 358 milioni di utenti
 - 2004 1,124 miliardi di utenti (213%)
- **Mailboxes**
 - 1999 315 milioni
 - 2004 678 milioni (115%)
- **Messaggi Email**
 - 1999 5,3 Miliardi al giorno
 - 2004 22,2 Miliardi (318%) al giorno

“Gli utenti executive spendono fino a 2,5 ore al giorno per la posta. L’Email è un’applicazione mission critical.”

SPAM



- **Cos'è**
 - ◆ Una marca di carne in scatola
 - ◆ Una sbobba generica
- **POSTA NON RICHIESTA**
 - ◆ Tipicamente per fini “commerciali”
 - ◆ Fenomeno legato alla diffusione della rete
 - ◆ Non diversa da quella che troviamo nella cassetta della posta

Come funziona

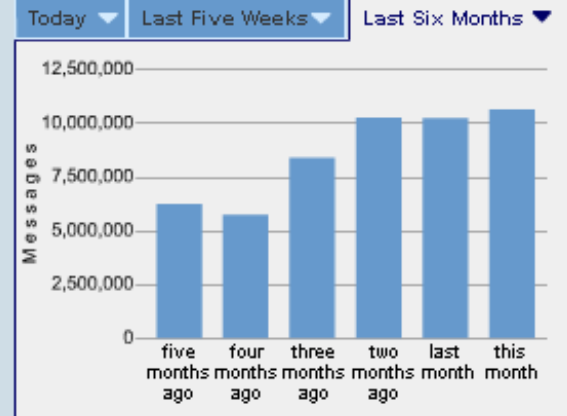


- **QUALCUNO RACCOGLIE INDIRIZZI DI POSTA (Directory Harvesting)**
 - ◆ **Solitamente li cede ad altri**

DHA Activity

An average of 30 percent of an email server's capacity is hijacked by spammers trying to steal proprietary email addresses and other information stored in the corporate directory. This technique is called a Directory Harvest Attack (DHA).

Successful DHAs can dramatically increase the volume of junk email (spam), forcing unprotected corporations and ISPs to incur higher email system costs and as well as decreased email system reliability.



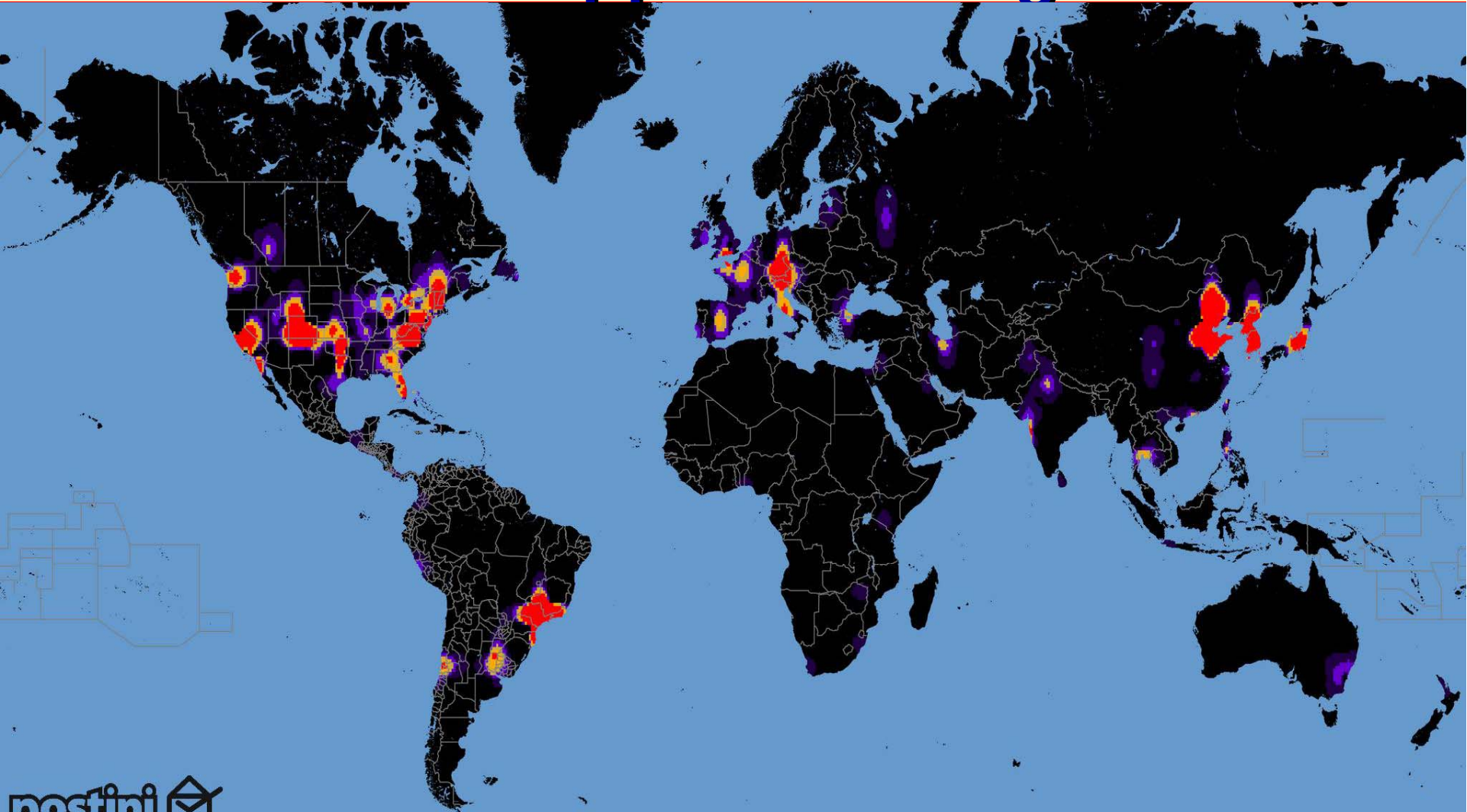
- **UN SISTEMA AUTOMATICO**
 - ◆ **Genera messaggi**
 - ◆ **Li invia a tutti gli indirizzi**

Da dove arriva



- **DA TUTTO IL MONDO**
 - ◆ Molto dagli USA
 - ◆ Molto dall'Asia
- **MA ANCHE DA NOI**
 - ◆ Da chiunque mandi messaggi in modo automatico
 - ◆ O metta in copia in modo esagerato
- **PERCHE'?**
 - Fini commerciali
 - Costa meno della posta tradizionale
 - Facile da attivare
 - Punta sulla quantità rispetto alla "qualità"
 - Nel mucchio qualcuno abbocca

Mappa delle origini (www.postini.com)



Perché è grave



- Perché assume proporzioni **gigantesche**
- Perché è veicolo di virus
- Perché viola la nostra privacy
- Perché invia contenuti discutibili
- Perché genera danno economico
 - Tempo di connessione
 - Spazio su disco
 - Tempo di analisi e cancellazione

Dati sullo SPAM

Spam Activity

Spam activity has increased over 65% since January, 2002. This increase causes email systems to experience unexpected overloads in bandwidth, server storage capacity, and loss of end-user productivity.

Today ▼

Types of Spam ▼

Last Five Weeks ▼

Last Six Months ▼

TOTAL SPAM IN PAST 24 HOURS:

Spam Messages: 104,229,286

Breakdown

Bulk Mail:	63.5 %
Special Offers:	30.9 %
Get Rich Quick:	2.1 %
Sexually Explicit:	3.4 %

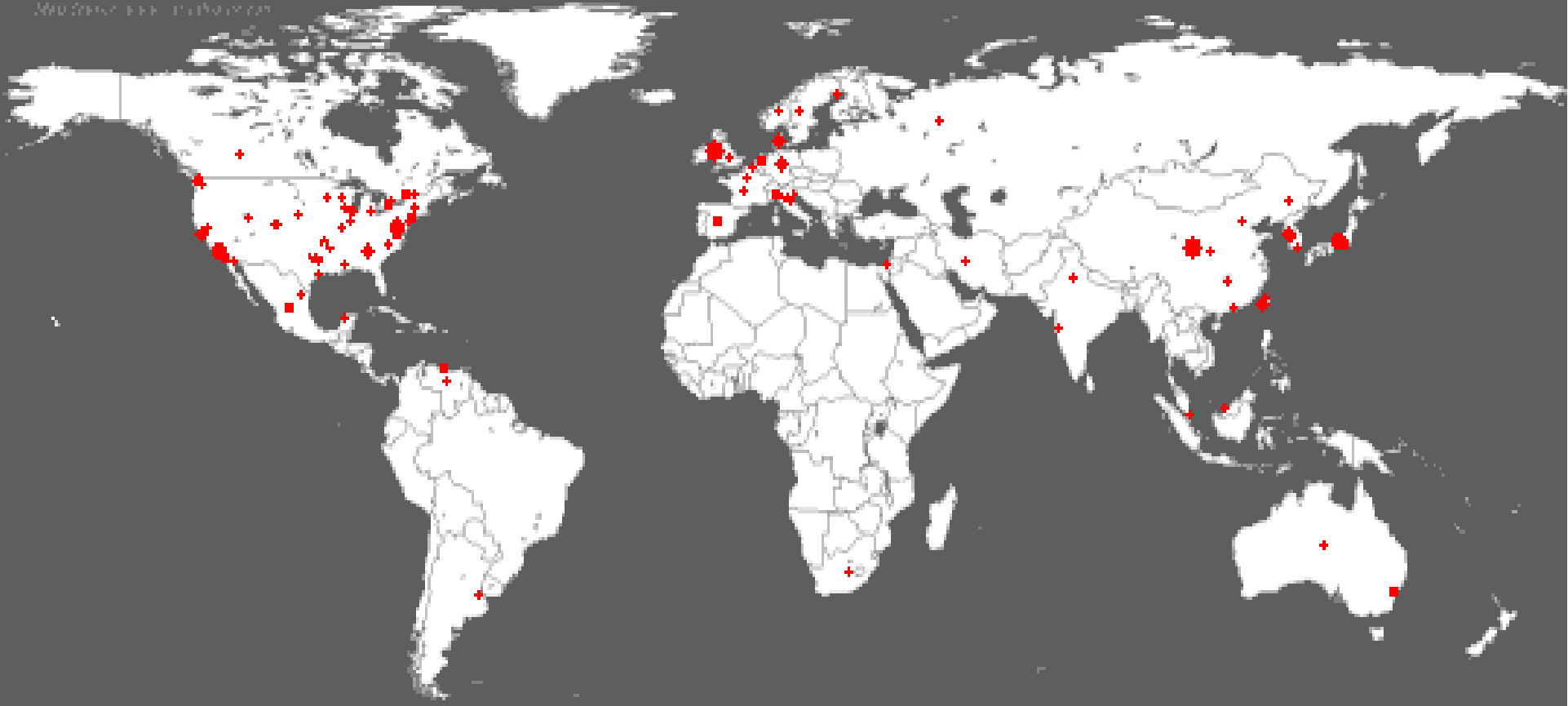
RECENT SPAM TOTALS:

Last 30 days: 2,809,717,729
13 terabytes

Last 6 months: 14,877,590,026
69.5 terabytes

La diffusione di Code Red

World map showing the distribution of Code Red



Thu Jul 19 00:00:00 2001 (UTC)

<http://www.caida.org/>

Victims: 159

Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

LA LEZIONE (www.caida.org)



- **Velocità e diffusione.**
- **In meno di 14 ore 359.104 computers compromessi.**
- **Danni minimi ma grande allarme (aveva timer di stop).**
- **Conteneva un DoS verso `www1.whitehouse.gov` e in modo non particolarmente scaltro (facile disattivazione).**
- **Non possiamo aspettarci altrettanta semplicità in futuro.**
- **Macchine anche di singoli utenti sono parte integrante della solidità complessiva della rete. Un computer vulnerabile mette tutti a rischio.**
- **E' una sveglia a mantenere i sistemi aggiornati: i pochi danni sono dovuti alla fortuna e non a una corretta gestione.**
- **Quanto velocemente è possibile informare?**
- **Ci serve proprio una catastrofe per capire? Il “baco” era stato scoperto il 18/6/2001 la prima versione di Code-Red appare il 12/7/2001 e la vera diffusione il 17 : ben 29 giorni!**

Slammer (Sapphire)



Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0

<http://www.caida.org>
Copyright (C) 2003 UC Regents

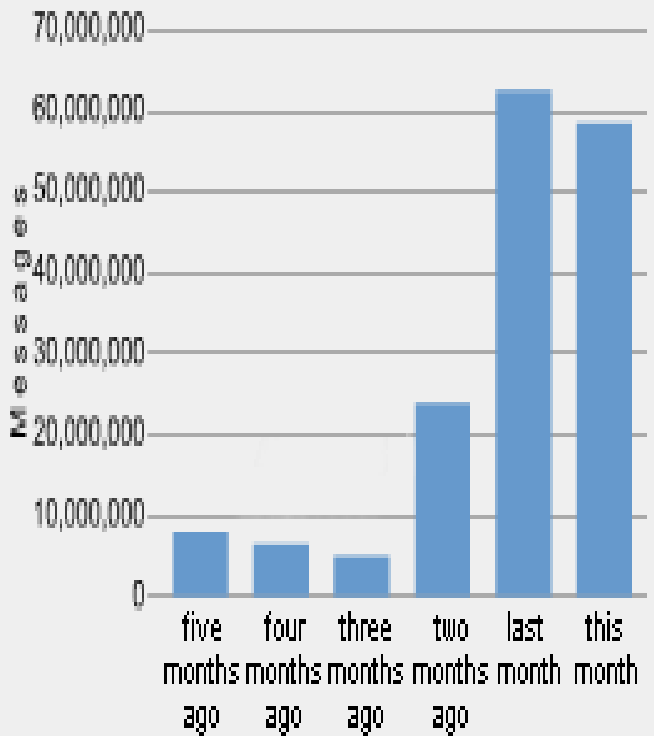
LA LEZIONE (www.caida.org)



- **Il worm Slammer si diffonde così rapidamente che la risposta umana è inefficace.**
 - Nel gennaio 2003 aveva un “carico” benigno ma la sua capacità distruttiva è stata potente
 - Slammer (chiamato anche Sapphire) è stato il worm più veloce della storia. Da quando ha iniziato a diffondersi in rete
- **ha infettato più del 90 % dei nodi vulnerabili in 10 minuti.**
 - Ha causato significativi danni a istituzioni finanziarie, di trasporto, governative, ha bloccato linee aeree, elezioni, ATM e servizi postali.
 - Slammer ha iniziato ad infettare i computer appena prima delle 05:30 UTC di sabato 25 gennaio 2003 sfruttando una vulnerabilità di buffer-overflow in computers che utilizzavano Microsoft SQL server o Desktop Engine 2000.
 - David Litchfield della Next Generation Security Software aveva scoperto e documentato questa vulnerabilità nel luglio del 2002; Microsoft aveva rilasciato la patch per la vulnerabilità prima che fosse pubblicamente resa nota (www.microsoft.com/security/slammer.asp).

Attacchi da virus

Today ▾
Today's Top Viruses ▾
Last Five Weeks ▾
Last Six Months ▾



Today ▾
Today's Top Viruses ▾
Last Five Weeks ▾
Last Six Months ▾

netsky	2,527,399
w32/netsky.q@mm	96,902
bagle	66,733
mydoom	45,595
klez	39,165
dumaru	38,571
w32/netsky.p@mm	21,814
w32/binnote@mm	10,501
netsky.p@mmlzip	9,676
swen	8,408
sobig	5,503
mimail	5,092
bagle.gen	3,998
urlspoo	3,545
bugbear	3,390
binnote	2,348
message_fragment	1,937
sircam	1,616
bagle.emlms03-032	1,014
w32/bagle.u@mm	929

Malware

- **Dai virus agli Exploit alla combinazione dei due**
- **BusinessWeek** Le due ultime vulnerabilità di Windows in agosto hanno causato danni stimati per 2 miliardi di dollari
- **Dialer**
- **Spyware**
- **Adware**
- **Popups**
- **Modifiche dei files di registro**
- **WORM**
- **NETWORK WORM**



Affrontare i worm



- Rispetto ai virus ha fattori di propagazione più alti
- Colpisce strutture delicate (server / apparati)
- Vanifica l'aumento di banda
- Genera crisi da infarto: passaggio repentino da funzionamento a blocco totale

Due approcci



- **In emergenza**, l'esigenza è di liberarsene al più presto e nel contempo limitarne quanto più possibile l'influenza
- **In esercizio** è invece indispensabile il loro rilevamento
 - Possibilmente evitandone l'ingresso nell'infrastruttura

Un problema per l'impresa



- Fermi macchina
- Perdite di operatività
- Intrusione
 - ◆ Spionaggio
 - ◆ Danneggiamento
- Danni a terzi
- **CREDIBILITA'**
- **COSTI**

SECONDO PUNTO

**Le infezioni saranno
sempre più gravi
nessuno potrà dirsi
immune**

Uno sguardo avanti

■ HIPERMOBILE

- ◆ GSM GPRS
- ◆ UMTS
- ◆ Wi-Fi

■ BROADBAND

- ◆ Canone, senza canone, gratis?



Advertisement for Alice services, featuring various plans like Alice Free, Alice Mega, Alice Flash, Alice Sat, and Alice Ricaricabile. It also shows a website interface with navigation options like 'I VANTAGGI DI ALICE', 'LE OFFERTE DI ALICE', and 'VERIFICA LA COPERTURA'.



Two advertisements for Adsl services. The first is 'Adsl SENZA CANONE' with the headline 'Tiscali libera anche Internet veloce' and 'Dai soli consumi, che consumi'. The second is 'Adsl SEMPRE' with the headline 'On line quando e quanto vuoi' and 'Tutto il giorno ad alta velocità'.



Advertisement for Fastweb services, featuring the headline 'ABBONATI ONLINE' and three service options:

INTERNET SENZA LIMITI	TV DI FASTWEB	TUTTO SENZA LIMITI
INTERNET SUPER VELOCE 24 ORE SU 24 ORE A	LA VERA TV INTERATTIVA (CON IL CALCIO GRATIS) A SOLI	INTERNET E TELEFONO ALL INCLUSIVE!
67 EURO	30 EURO	85 EURO

Velocità e rischio



- **Vendere solo la velocità è sbagliato**
- **Il rischio di infezione aumenta esponenzialmente**
- **L'attacco distribuito da milioni di utenti ignari (in larga banda)**
 - ◆ **È come dare un cannone a tutti**

La riflessione



- La soluzione delle problematiche di sicurezza è **CONDIZIONE** per lo sviluppo di nuovi sistemi informativi on-line

La posta in gioco



- **Non sono in gioco i bit e i bytes**
- **E' in gioco il sistema nervoso dell'impresa**
- **E' in gioco la difesa della nostra privacy**
- **Non basta la tecnica**
- **Occorre organizzazione**
- **Non basta la buona volontà**
- **Occorre la disciplina**

Sicurezza e etica



- Sicurezza non per paura
- Sicurezza non per chiudere

- SICUREZZA PER
DARE SICUREZZA

Come difendersi



- In fondo con il “tasto magico” risolvo senza grandi fatiche
- Non aprire SPAM per nessun motivo (è come grattarsi con l’orticaria)
- Non rispondere MAI
- Meglio disattivare la “anteprima”
- Con la conoscenza
- I software di filtro
- Ambienti protetti
- Sistemi di controllo centrali
- Attivazione di regole personali

Riconoscere lo SPAM



- **Nessun mio amico mi scrive “urgente per gigi@siosistemi.it”**
- **E’ strano se vostra mamma vi scrive in inglese e vi invita a comperare viagra...**
- **Gli Spammers sono sempre più creativi**
 - Messaggi di finta replica
 - Messaggi con mittenti “credibili”
 - Parole chiave scritte in modo particolare

Web con filtro o senza?



- **Controllare l'uso di Internet per i rischi associati**
 - ◆ Tutela nelle scuole
- **Costi per produttività e rispetto della legalità**
 - ◆ 70% della pornografia in rete si consuma tra le 9 e le 17
 - ◆ Più del 60% degli acquisti in Internet avvengono in orari di lavoro
- **Ottimizzare l'uso della banda**
 - ◆ 30-40% del surfing in rete non riguarda il business

Internet Content Security



- **Controllare e bloccare SPAM, virus e worm**
- **Bloccare l'accesso a siti non autorizzati**
- **Controllare il tipo e le dimensioni dei files che vengono scaricati**

Un'"analisi del colesterolo"



- Installazione di una sonda su un segmento significativo della rete
- Campionatura del traffico
- Acquisizione dei risultati
- Analisi e relazione
- Azioni di profilassi



**La sicurezza
è fondamentale
una questione di
persone**

Grazie per l'attenzione

gigi@siosistemi.it