



USO DELLA POSTA ELETTRONICA

ASPETTI NORMATIVI,
RISCHI TECNICI,
PROTEZIONE ED USO SICURO

SECURITYNET®
SERVIZIO ANTIVIRUS E PREVENZIONE COMPUTER CRIME.

 **Club sul Computer Crime**

GRUPPO

BANCHE
POPOLARI

e-mail storia

1971

Cambridge, Massachusetts, USA.
Appalto alla *Bolt Beranek and Newman*
per lo sviluppo operativo di Arpanet



Ray Tomlinson scrive 200 righe di codice
che danno inizio alla rivoluzione

Il software, scritto per un sistema di *time sharing*,
era diviso in 2 parti:

1. SENDMSG per spedire i messaggi,
2. READMAIL per riceverli.

Oltre a: CPYNET un protocollo per trasferire file.

1972

La *Hobbes Timeline Tomlinson* perfeziona l'invenzione
Inserendo la “@” commerciale.

e-mail storia

- 1973 Primo protocollo di trasferimento
- 1990 12 milioni di indirizzi di posta elettronica su BBS
- 1993 Mosaic. E' il via alle attuali e-mail
- 1994 Netscape
- 1997 Outlook
- 2000 505 milioni di indirizzi
- 2002 Scambiati 30 miliardi di messaggi al giorno
- 2004 19 milioni di italiani usano Internet e scambiano e-mail
- 2004 **Prima sentenza in Italia di risarcimento danni per *spamming***
Napoli 24 Giugno. € 1.000,00 di danni patrimoniali e morali, € 750,00 di spese, pubblicazione della sentenza su Corriere della Sera, La Repubblica, Il Giornale, Il Messaggero, Panorama ed Espresso.

Origine del grafema @



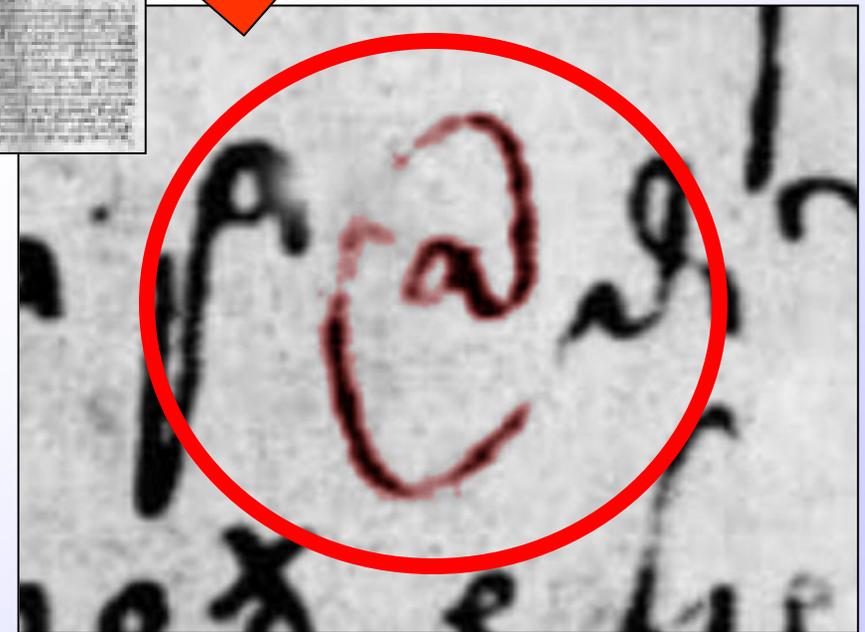
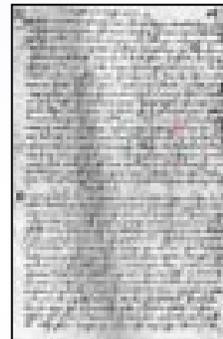
Per *Ray Tomlinson*, inventore delle e-mail, era uno dei segni della tastiera non utilizzati per scrivere nomi e significava “at”, “presso”

Nel secolo scorso “at”
assunse un uso commerciale,
come abbreviazione: “*at price off*”

Ma il grafema appare già in una lettera
commerciale del 4 maggio 1536.

È usato dai veneziani della Serenissima
come abbreviazione della parola ANFORA
unità di misura di peso antichissima.

Nel 1492 un dizionario Spagnolo-Latino
traduce la parola ANFORA in ARROBA,
analoga unità di misura del mondo
arabo ispanico.





USO DELLA POSTA ELETTRONICA

**ASPETTI NORMATIVI,
RISCHI TECNICI,
PROTEZIONE ED USO SICURO**

SECURITYNET®
SERVIZIO ANTIVIRUS E PREVENZIONE COMPUTER CRIME

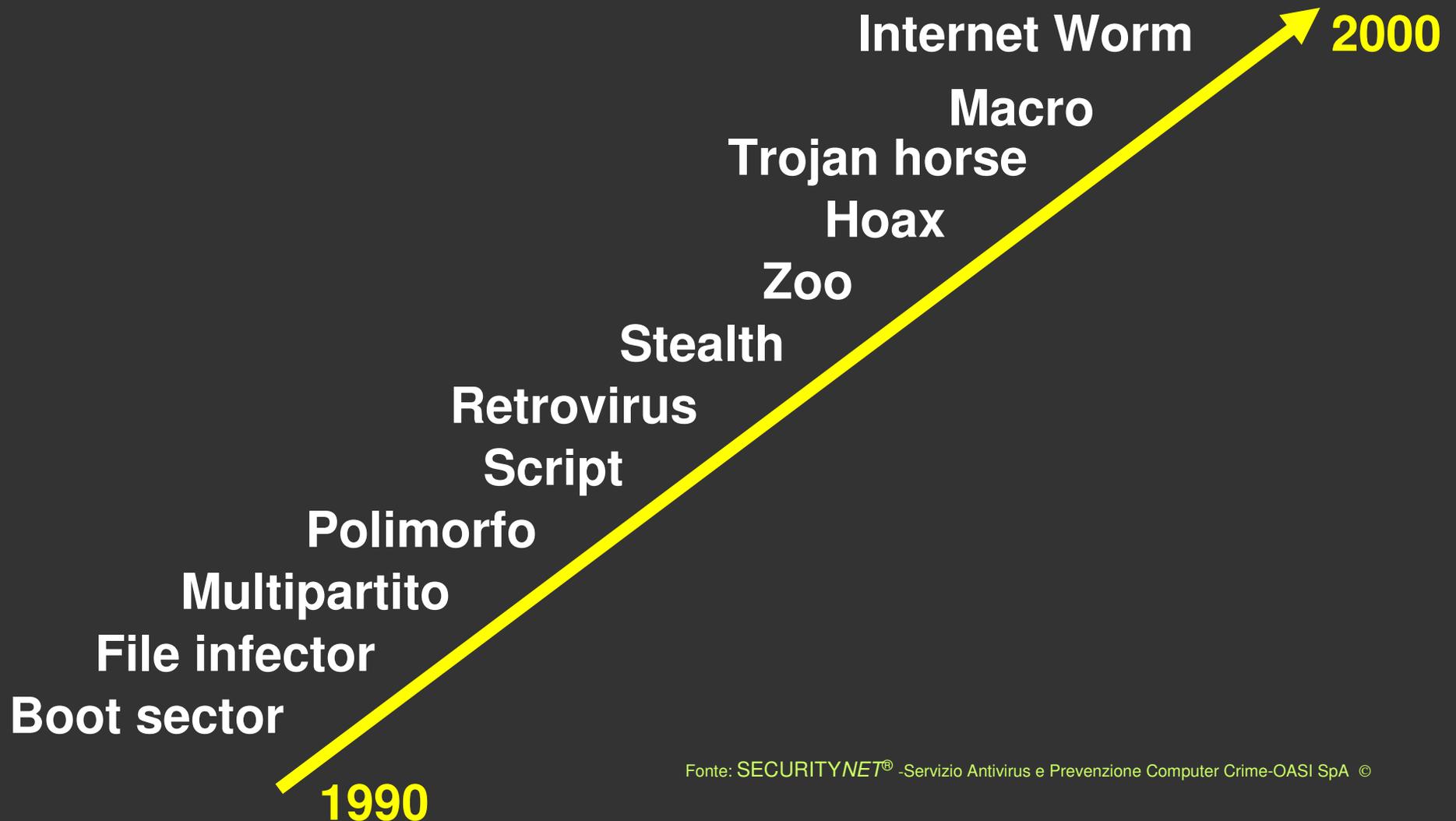
CC
Club sul Computer Crime

LA RICERCA SECURITYNET 2004 L'INCIDENZA DI E-MAIL WORM, NETWORK-WORM E VULNERABILITA' NELLA PROTEZIONE DEI DATI

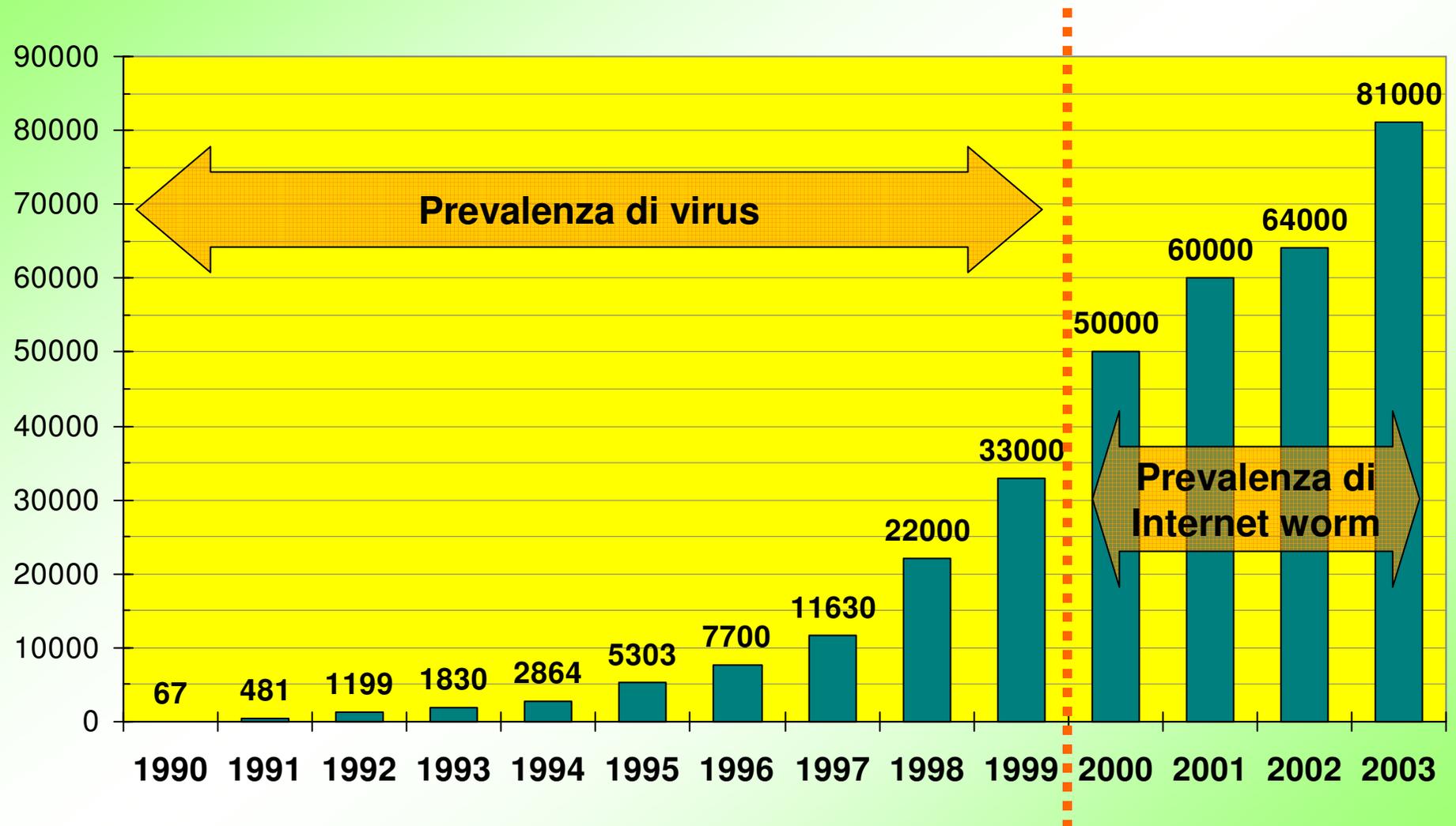
- Aspetti storici
- Statistiche
- Nuove tendenze
- Aspetti legali



I virus cambiano nel tempo e sono classificati in base agli oggetti infettati ed alle tecniche di infezione.



NUMERO DI VIRUS NEL MONDO dal 1990 al 2003

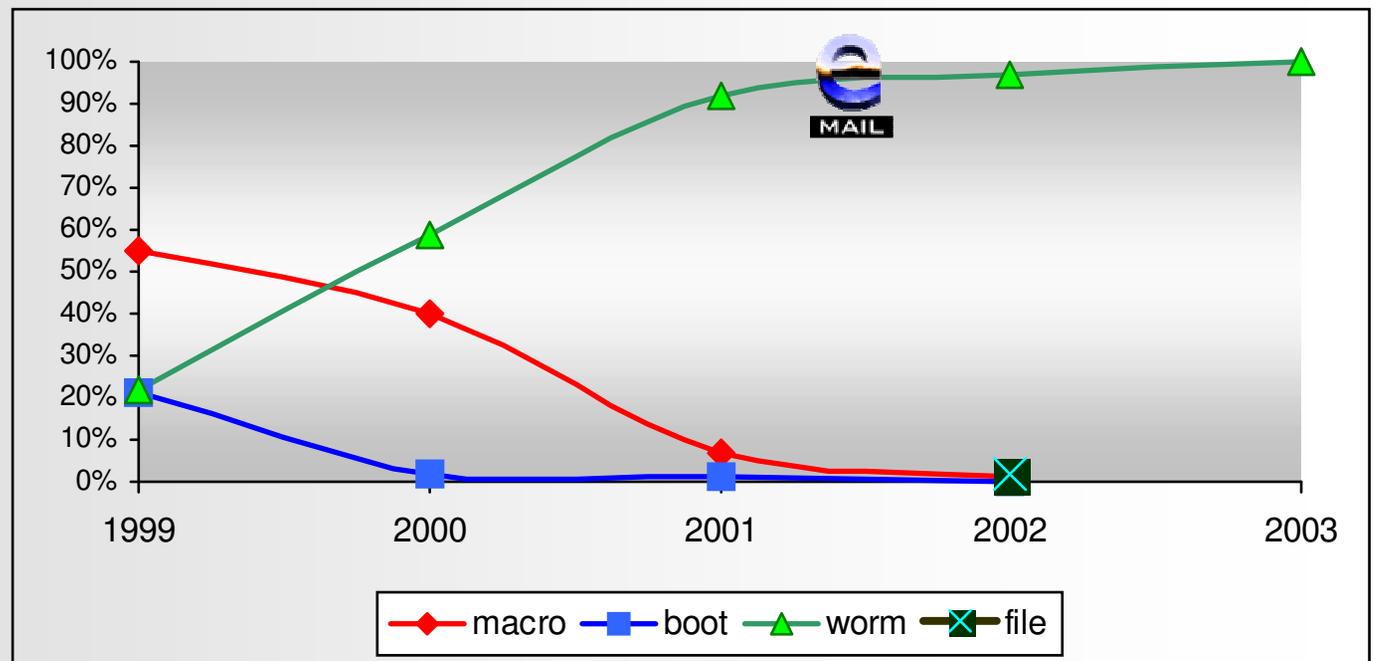
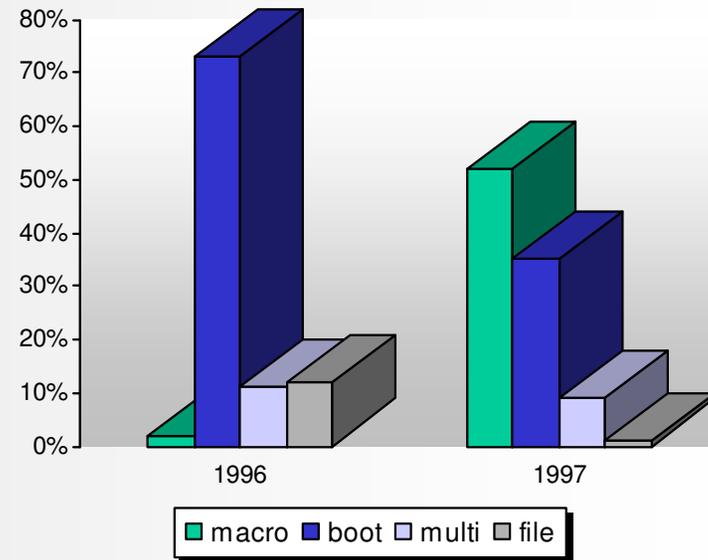


Fino al 1996 prevalgono i virus di boot.

Dal 1997 l'avvento dei macrovirus.

Dal 1999 inizia la crescita degli Internet worm.

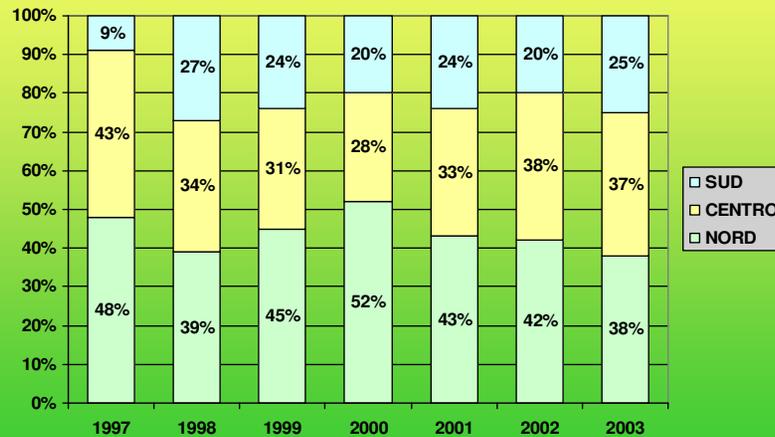
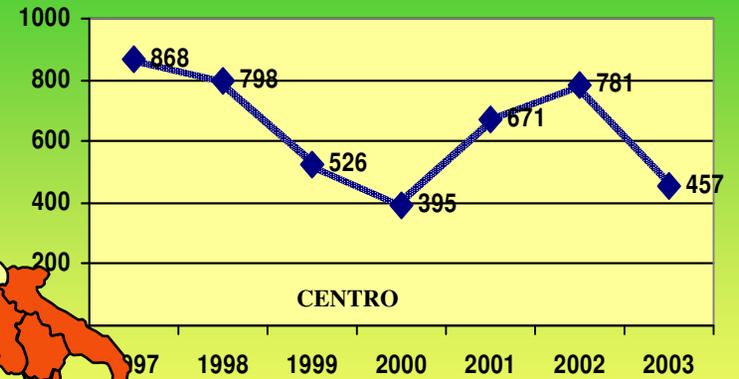
Dal 2000 quasi solo worm.



ANALISI DEGLI ANDAMENTI

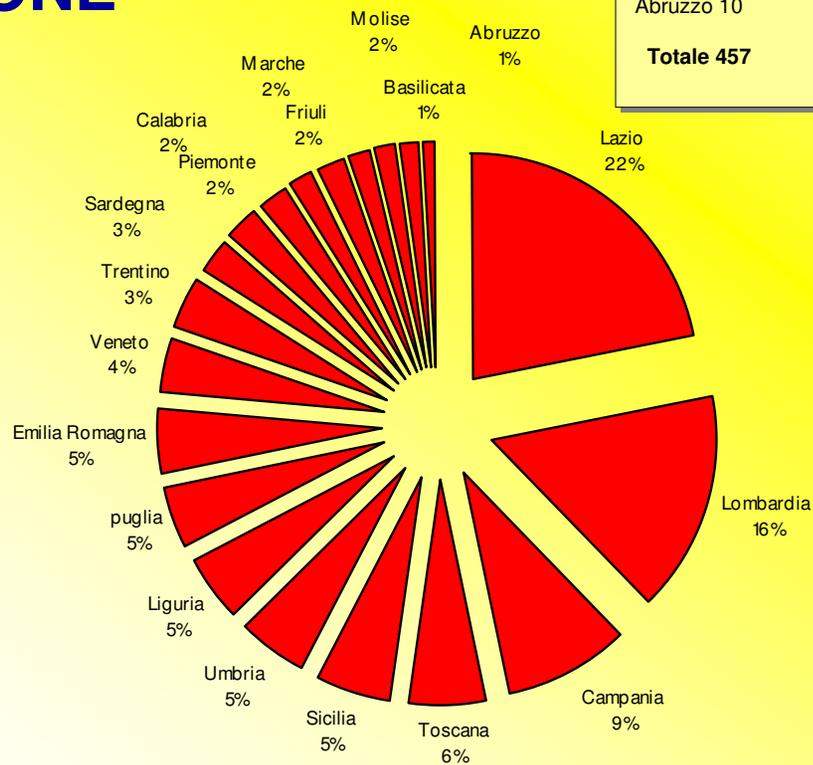
considerando 12.825 casi
segnalati a SecurityNet dal 1997 al 2003

REGIONE	1997	1998	1999	2000	2001	2002	2003	TOTALE	PERCENT
Abruzzo	21	93	68	34	97	50	10	373	2,91%
Basilicata	13	88	52	31	93	11	18	306	2,39%
Calabria	7	89	61	18	73	31	28	307	2,39%
Campania	41	119	76	34	74	175	113	632	4,93%
Emilia Romagna	113	115	89	52	70	98	57	594	4,63%
Friuli	24	91	67	31	56	25	23	317	2,47%
Lazio	636	169	130	171	161	358	275	1.900	14,81%
Liguria	26	97	86	46	112	92	59	518	4,04%
Lombardia	417	181	186	343	188	308	198	1.821	14,20%
Marche	32	107	66	43	100	91	22	461	3,59%
Molise	60	92	59	30	85	39	21	386	3,01%
Piemonte	264	135	141	120	154	170	31	1.015	7,91%
Puglia	29	99	104	101	99	83	58	573	4,47%
Sardegna	24	106	66	54	77	53	32	412	3,21%
Sicilia	60	122	59	41	80	52	66	480	3,74%
Toscana	100	247	123	62	132	153	69	886	6,91%
Trentino	27	98	51	32	58	27	43	336	2,62%
Umbria	19	90	80	55	96	90	60	490	3,82%
Val d'Aosta	10	94	51	38	81	20	18	312	2,43%
Veneto	90	100	106	66	163	130	51	706	5,50%
	2.013	2.332	1.721	1.402	2.049	2.056	1.252	12.825	100,00%



DISTRIBUZIONE GEOGRAFICA DEI CASI segnalazioni di virus in aziende rilevati da SecurityNet dal 1997 al 2003

ANNO 2003 NUMERO DI WORM SEGNALATI PER OGNI REGIONE



CENTRO 37%

Lazio 275
Toscana 69
Umbria 60
Marche 22
Molise 21
Abruzzo 10

Totale 457

NORD 38%

Lombardia 198
Liguria 59
Emilia Romagna 57
Veneto 51
Trentino 43
Piemonte 31
Friuli 23
Val d'Aosta 18

Totale 480

SUD 25%

Campania 113
Sicilia 66
Puglia 58
Sardegna 32
Calabria 28
Basilicata 18

Totale 315

DIFFUSIONE DEI VIRUS DURANTE L'ANNO

MESI	1998	1999	2000	2001	2002	2003	Totale	Percent.
Gennaio	123	71	59	118	52	93	516	3%
Febbraio	231	144	75	51	70	34	605	3%
Marzo	214	167	78	103	169	102	833	8%
Aprile	193	170	76	91	255	49	834	12%
Maggio	214	162	290	70	246	75	1.057	12%
Giugno	225	178	102	92	86	190	873	4%
Luglio	133	109	66	267	176	52	803	9%
Agosto	112	90	71	108	64	120	234	3%
Settembre	124	98	129	365	59	226	1.001	3%
Ottobre	233	153	80	289	448	188	1.391	22%
Novembre	244	171	211	261	304	80	1.271	15%
Dicembre	286	208	165	234	127	43	1.063	6%
Totale	2.332	1.721	1.402	2.049	2.056	1.252	10.481	100%

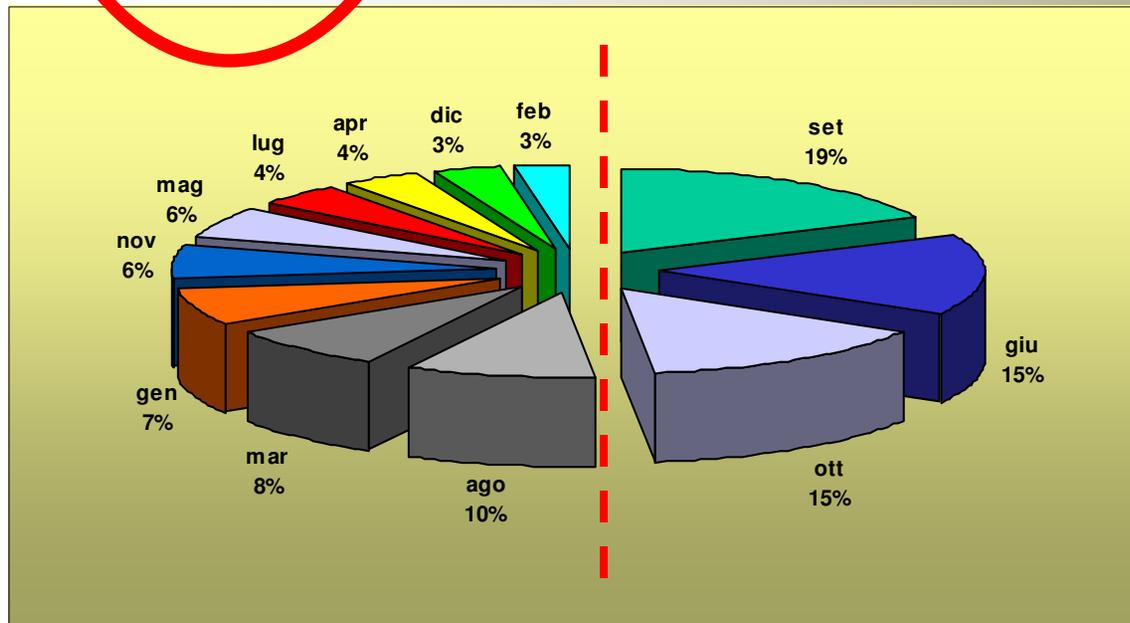
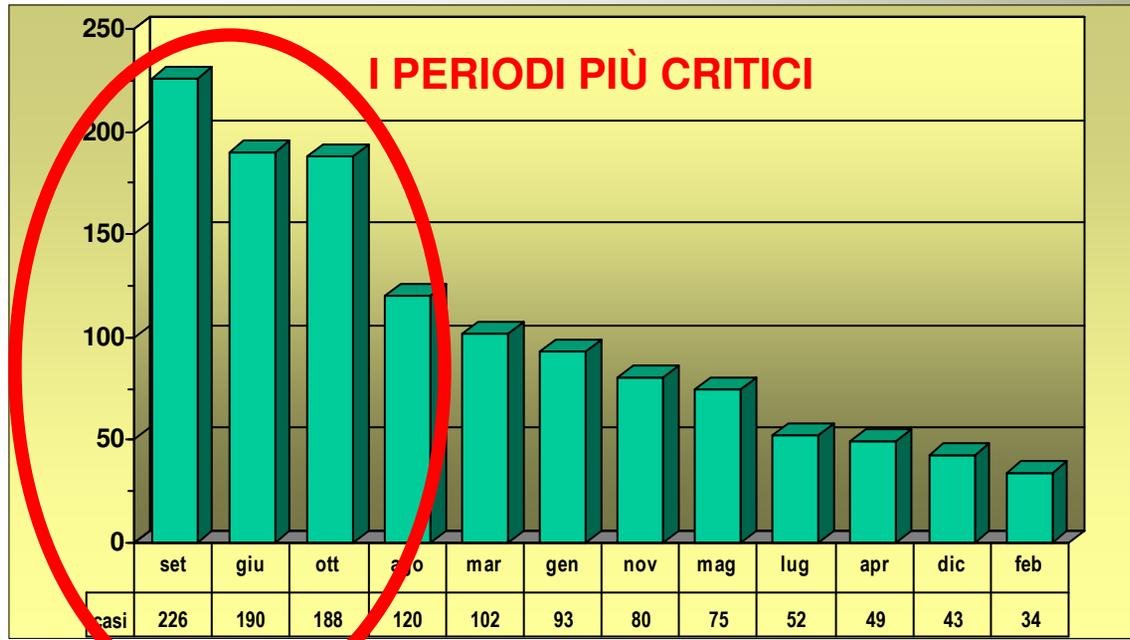
DIFFUSIONE DEI VIRUS DURANTE L'ANNO



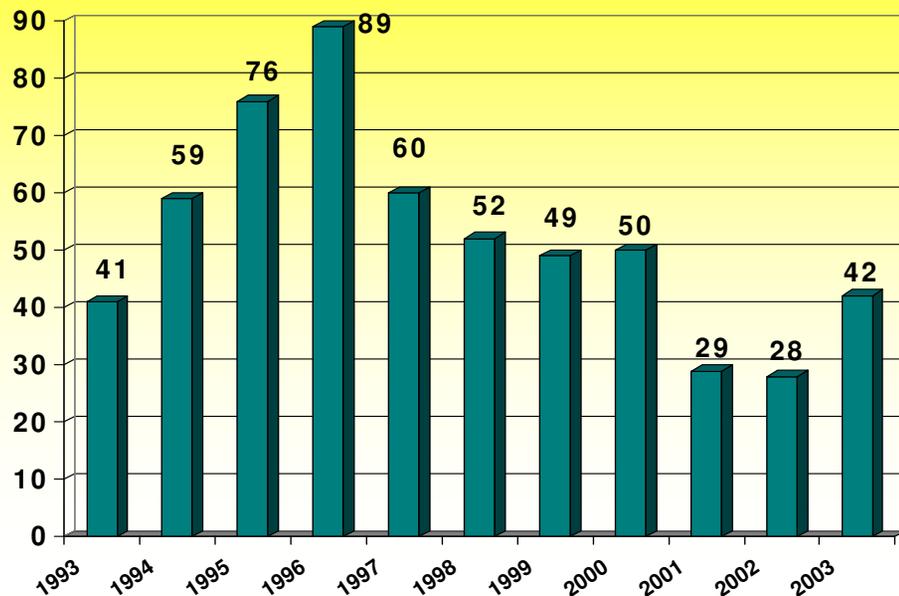
■ Gennaio
 ■ Febbraio
 ■ Marzo
 ■ Aprile
 ■ Maggio
 ■ Giugno
 ■ Luglio
 ■ Agosto
 ■ Settembre
 ■ Ottobre
 ■ Novembre
 ■ Dicembre

ANNO 2003

NUMERO DI
WORM
SEGNALATI
OGNI MESE



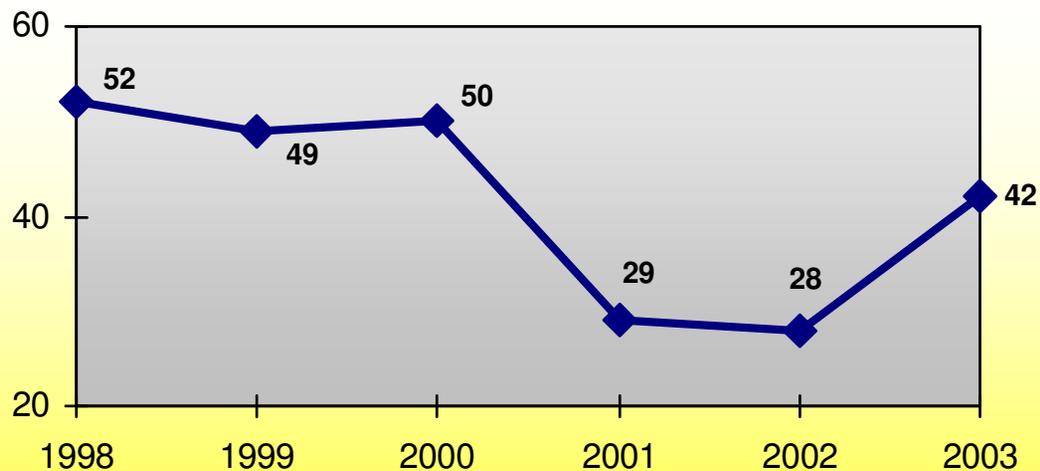
N. DI VIRUS PRINCIPALI DIFFUSI IN ITALIA



**QUANTITA'
DEI DIVERSI
TIPI DI VIRUS
CHE HANNO
PROVOCATO
INFEZIONI E
INCIDENTI
IN ITALIA**

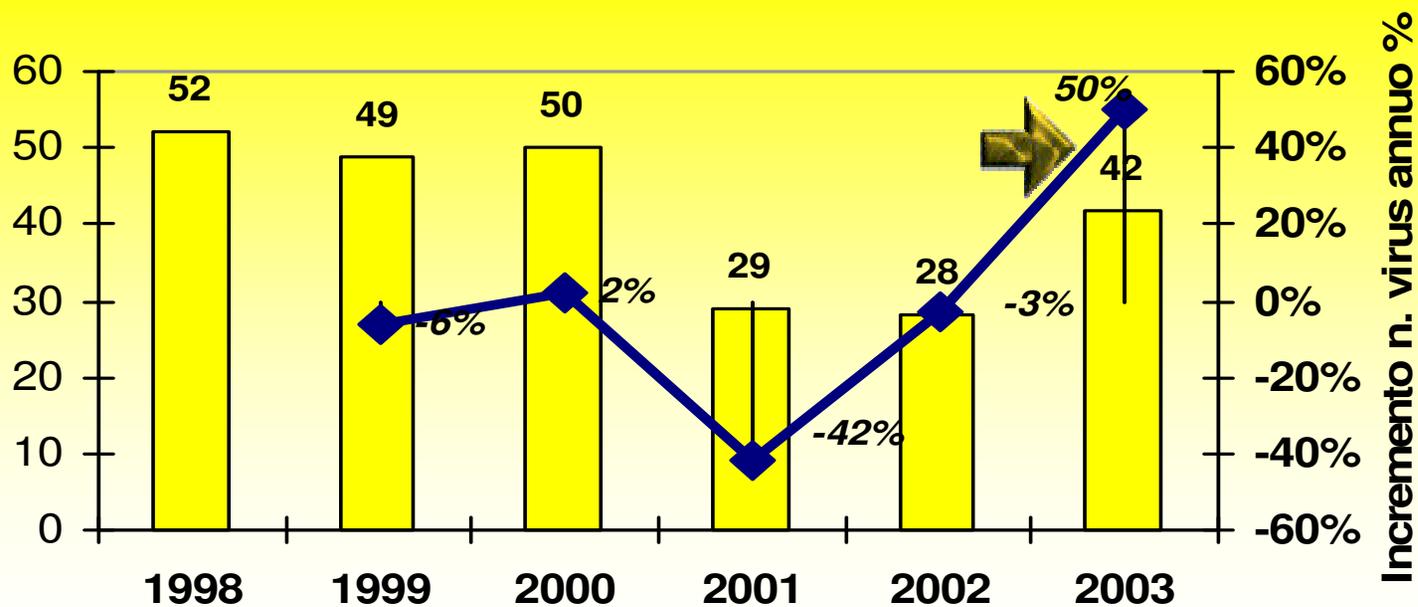
TIPI DI VIRUS DIFFUSI IN ITALIA



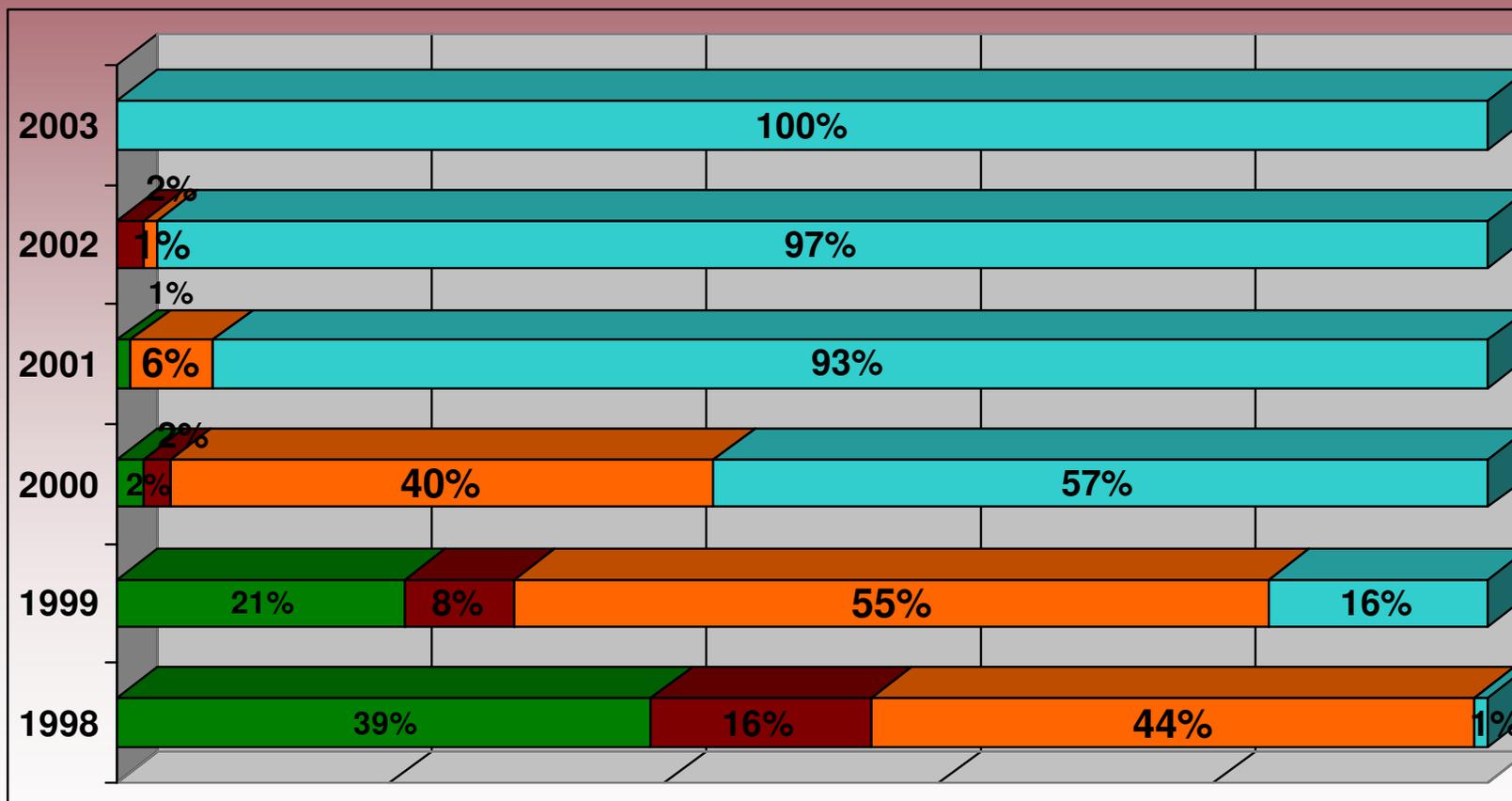


ANDAMENTO DELLA QUANTITA' DEI DIVERSI TIPI DI VIRUS CIRCOLANTI IN ITALIA DAL 1998 AL 2003

TIPI DI VIRUS PIU' DIFFUSI E INCREMENTO SULL'ANNO PRECEDENTE



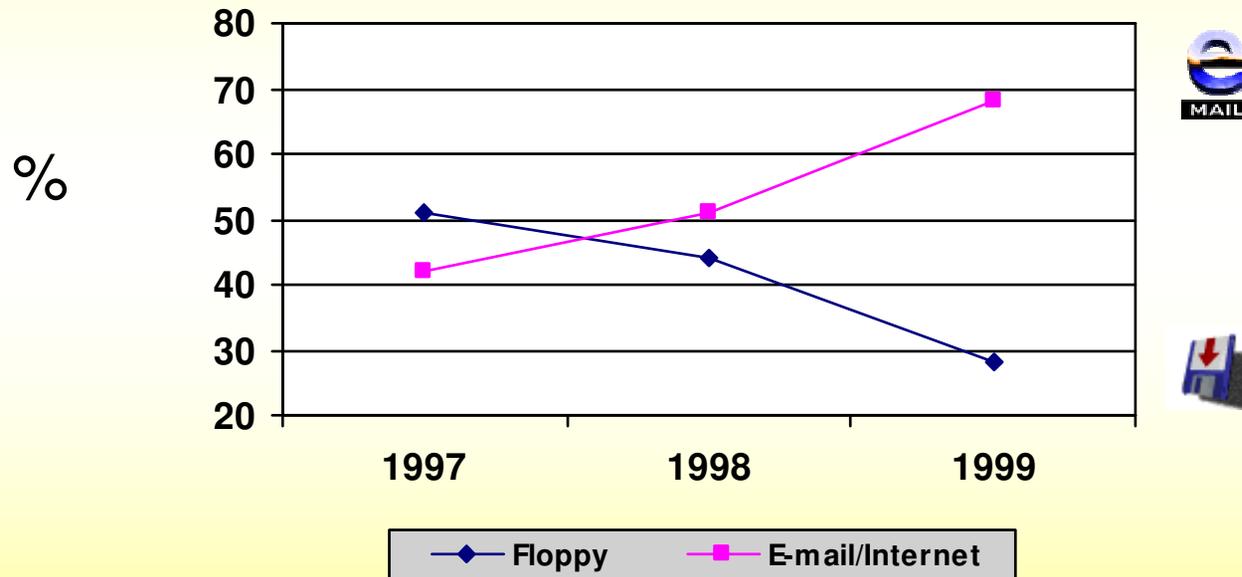
INCIDENZA DELLE DIVERSE TIPOLOGIE DI VIRUS SUL TOTALE DELLE INFEZIONI RILEVATE IN ITALIA DA SECURITYNET DAL 1998 AL 2003



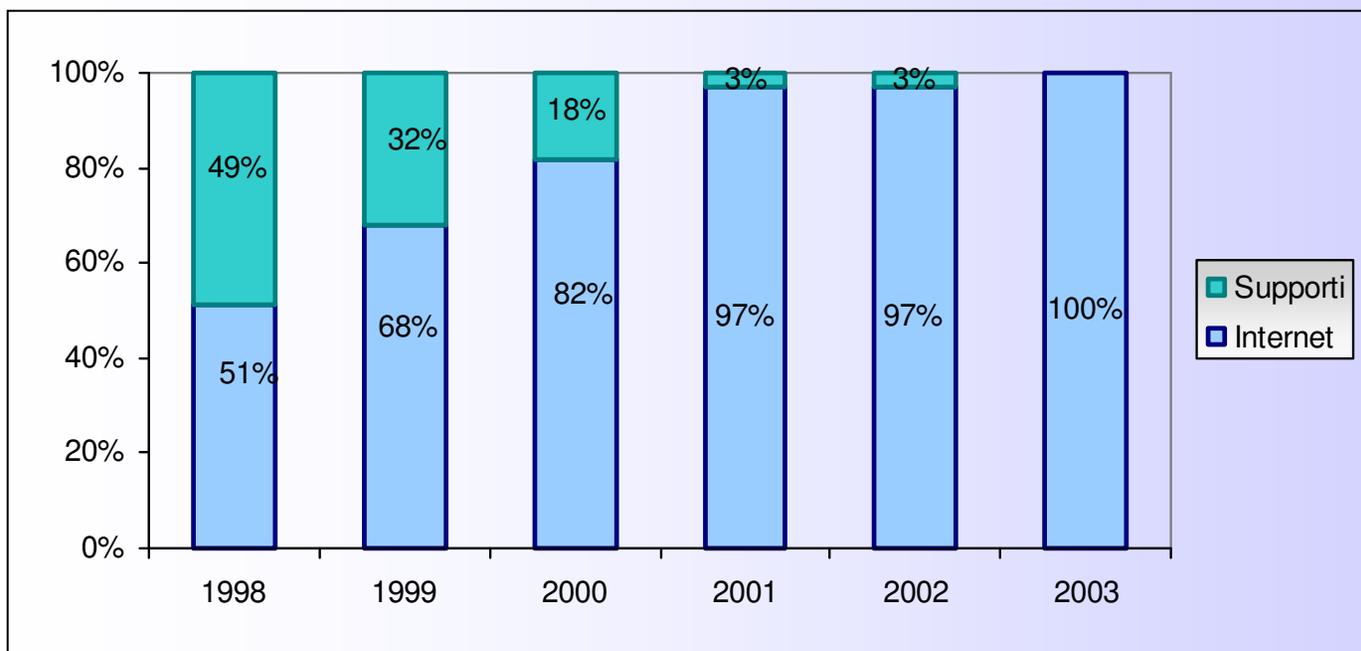
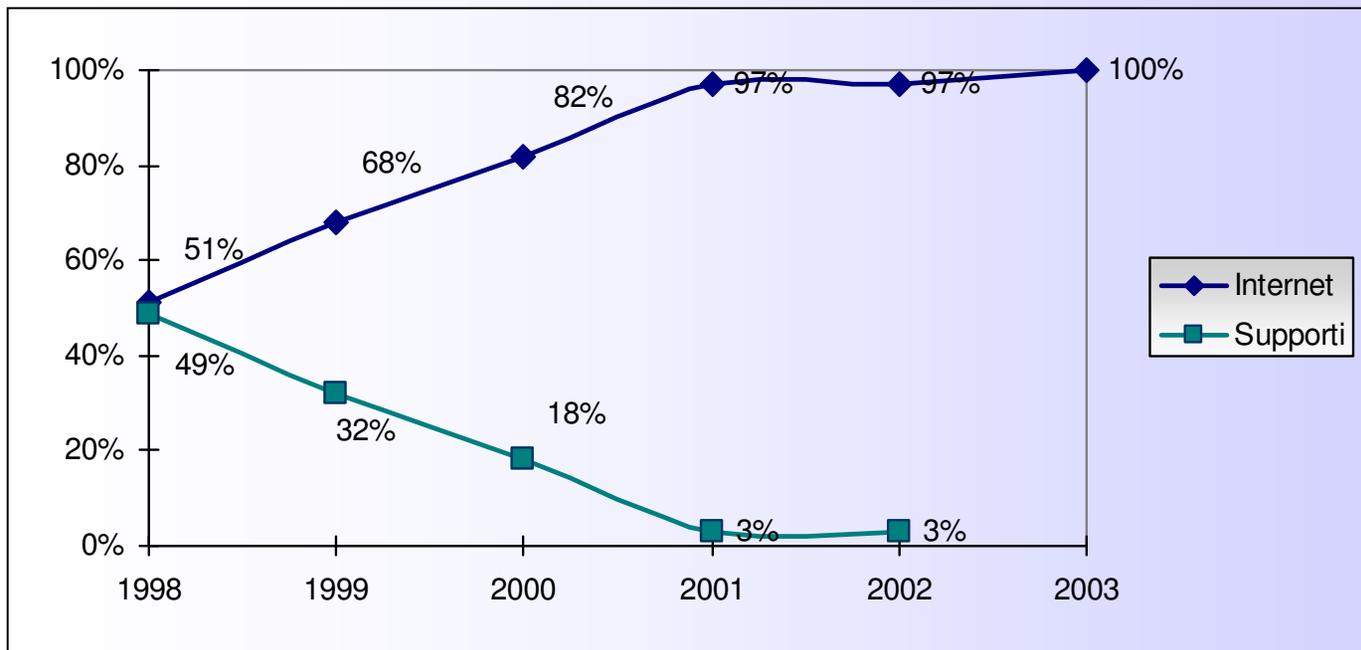
■ Boot ■ File ■ Macro ■ Worm

ANDAMENTO DEI MEZZI DI PROPAGAZIONE DEI VIRUS

Fino al 1997 prevalgono i supporti (floppy disk e CD).
Dal 1998 inizia la prevalenza di Internet

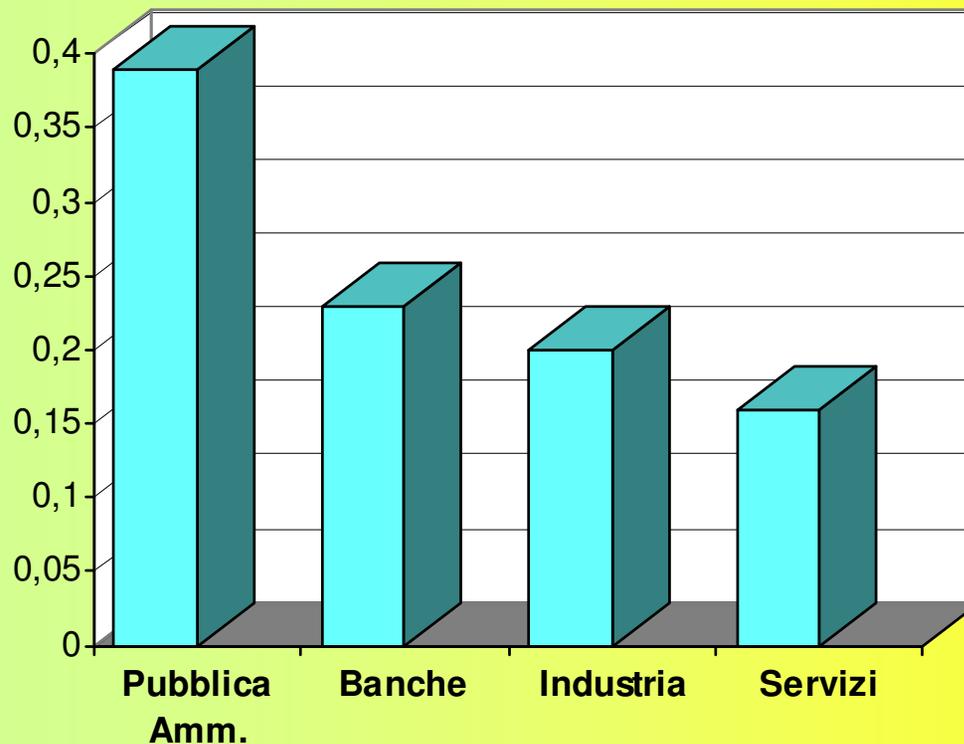


ANDAMENTO DEI MEZZI DI PROPAGAZIONE DEI VIRUS IN ITALIA DAL 1998 AL 2003



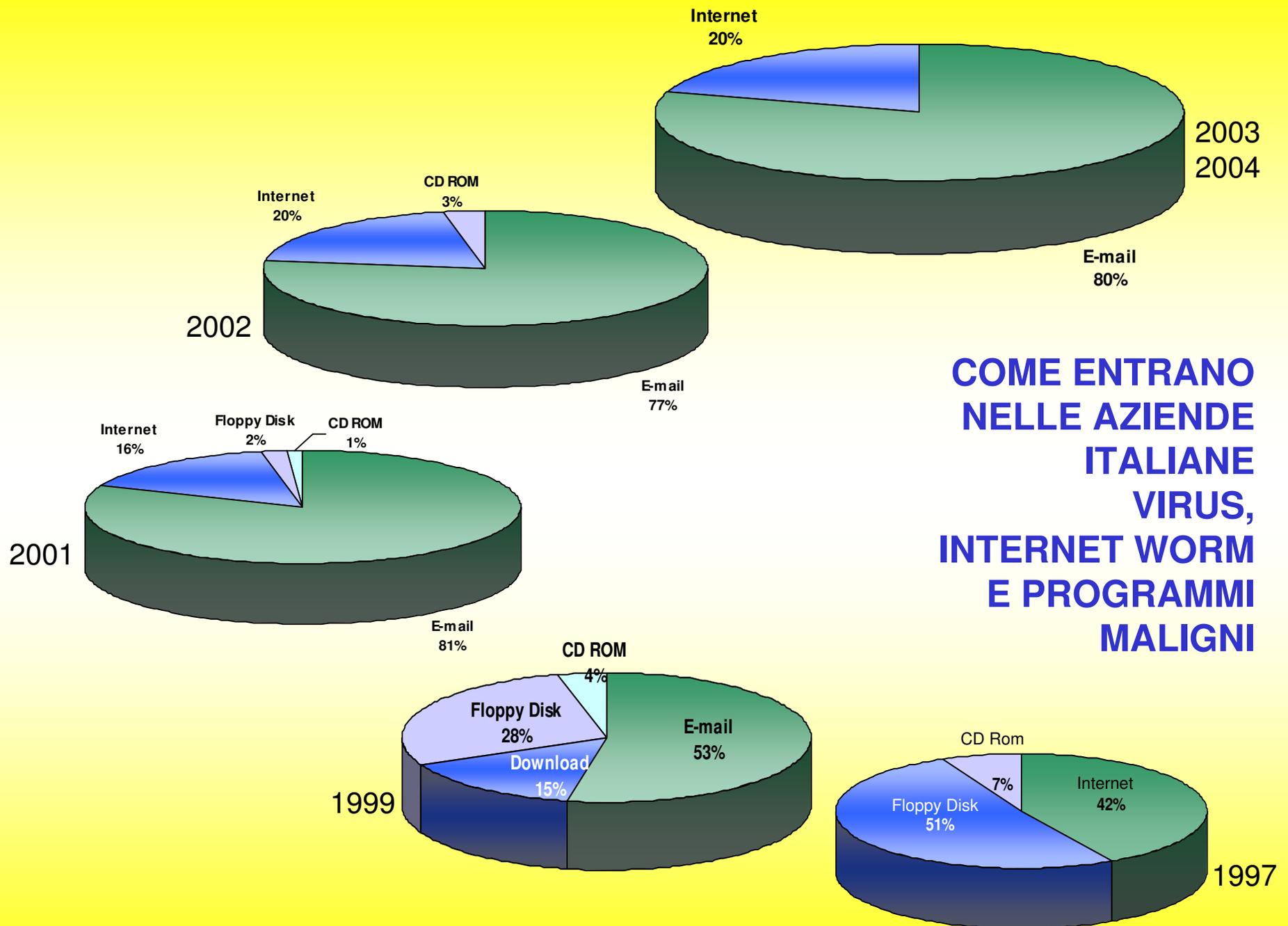
TEMPO MEDIO (tempo perso) DEDICATO DALLE AZIENDE AD OGNI INCIDENTE FINO AL 1997

Frazione di giorno
1 giorno = 7,5 ore



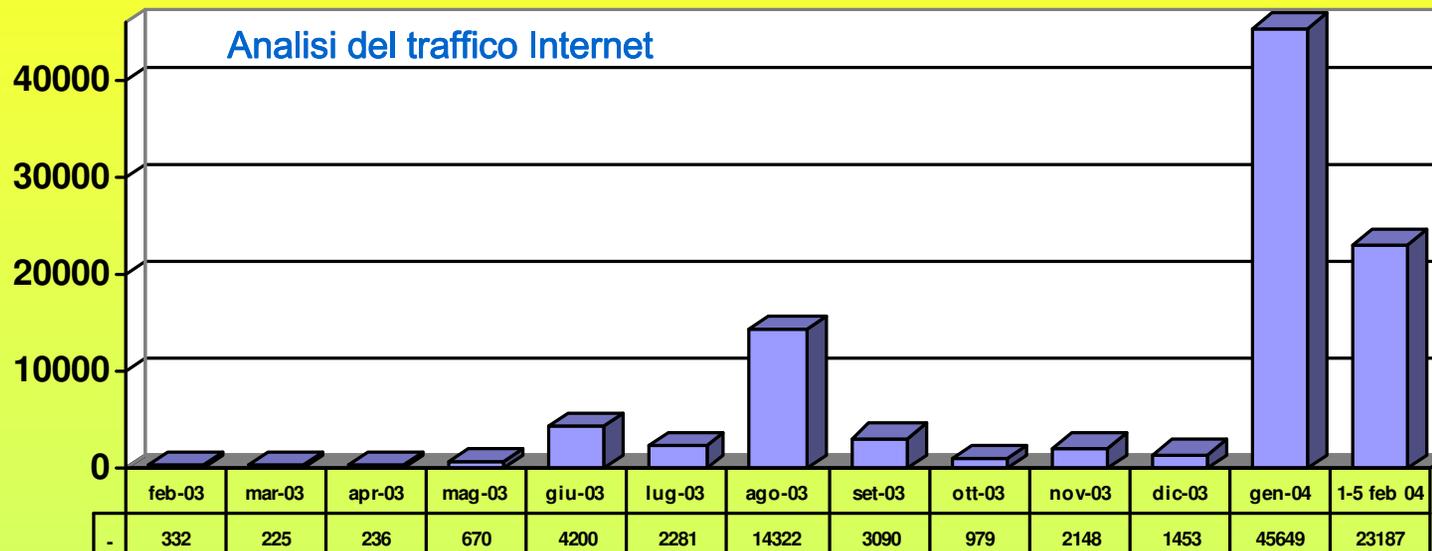
**Dal 2001
non si riscontrano significative differenze
tra le diverse categorie aziendali**

COME ENTRANO NELLE AZIENDE ITALIANE VIRUS, INTERNET WORM E PROGRAMMI MALIGNI



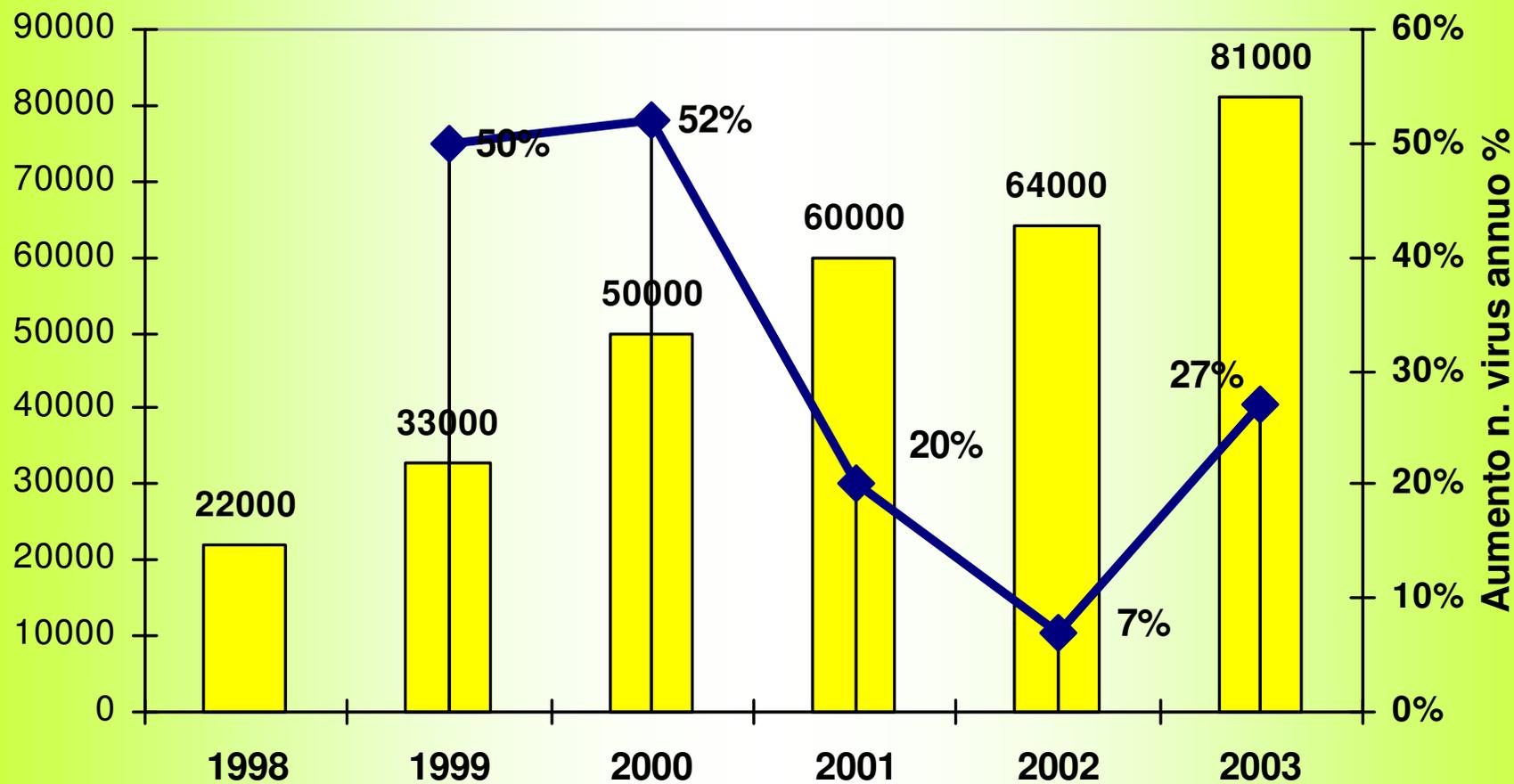
VIRUS INTERCETTATI IN UNA RETE DI 9.000 COMPUTER

Su una rete distribuita su tutto il territorio nazionale di circa 9.000 computer dal 2 febbraio 2003 al 5 febbraio 2004. Nei mesi di gennaio e inizio febbraio 2004 sono state bloccate 98.000 e-mail infette. Pari a 268 al giorno ed a 445 al giorno se proporzionati ai 220 giorni lavorativi convenzionali.



L'incidenza media riportata al numero di computer è stata di 11 virus l'anno (per ogni computer connesso alla rete).

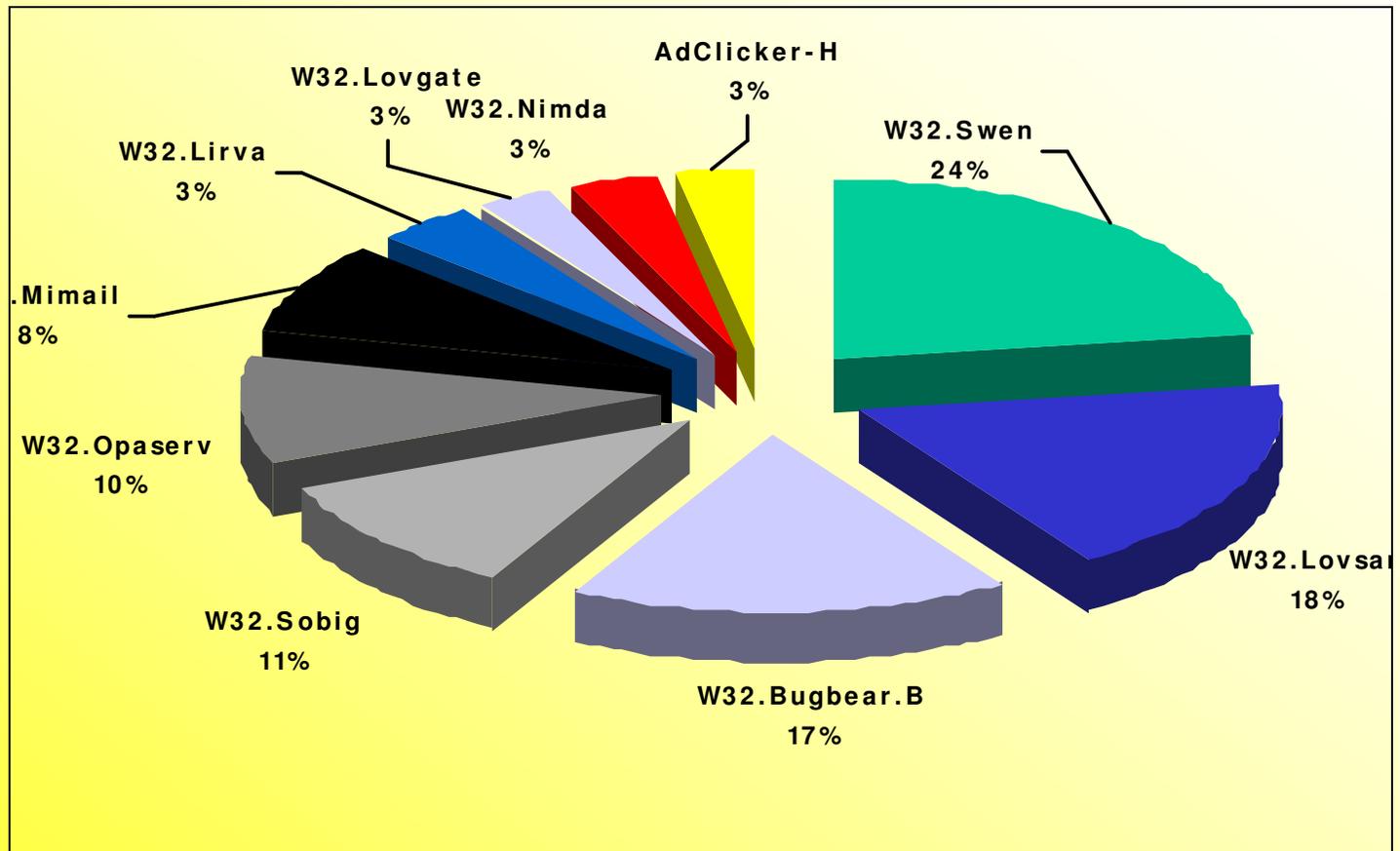
VIRUS NEL MONDO, QUANTITA' E INCREMENTO SULL'ANNO PRECEDENTE



**La nuova crescita dell'incremento annuale
rispetto all'anno precedente è dovuta ai network worm**

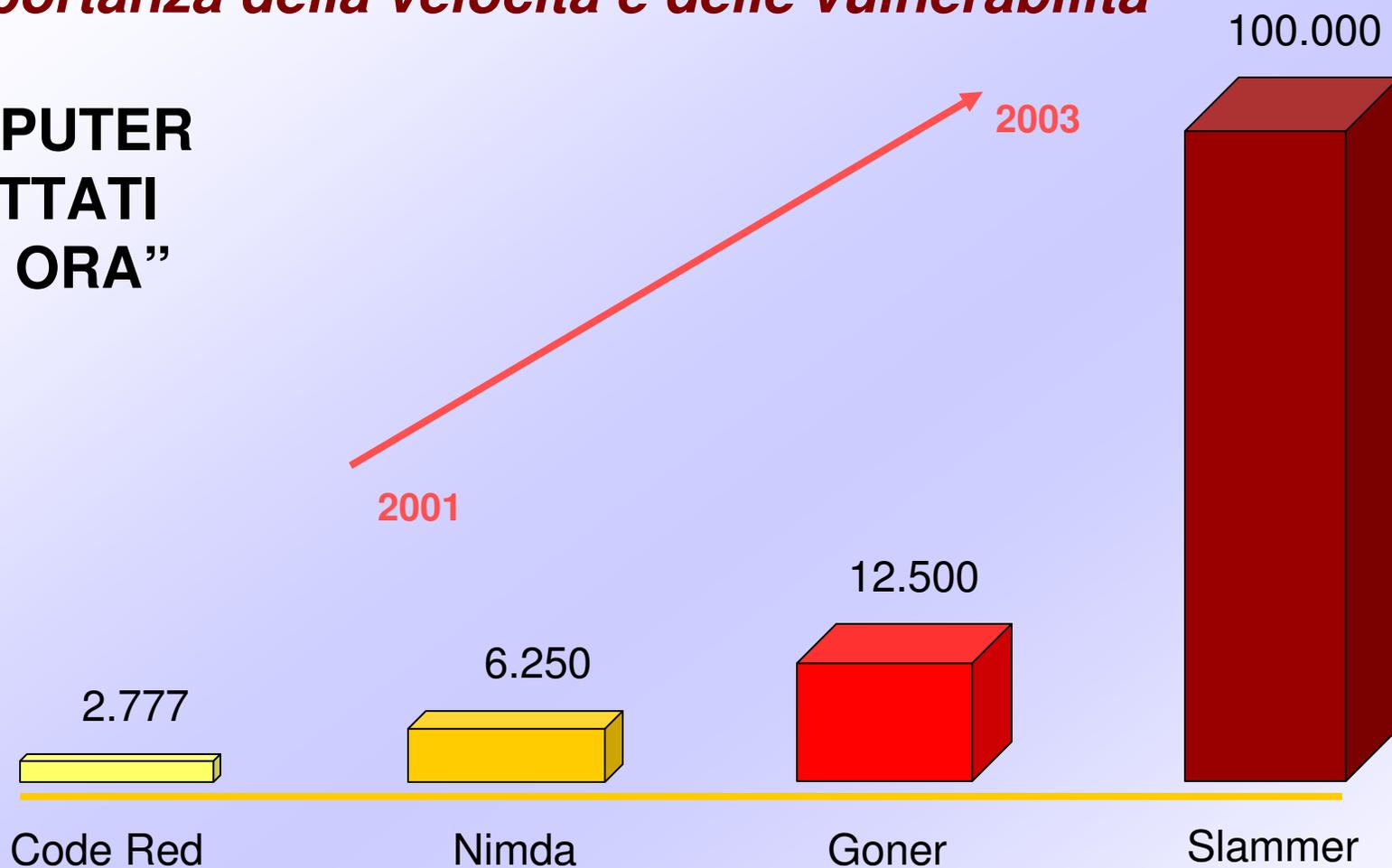
NEL 2003 DIECI INTERNET WORM HANNO GENERATO L'83% DEI CASI

W32.Swen	236
W32.Lovsan	187
W32.Bugbear.B	177
W32.Sobig	111
W32.Opaserv	102
W32.Mimail	88
W32.Lirva	36
W32.Lovgate	34
W32.Nimda	33
AdClicker-H	32



L'importanza della velocità e delle vulnerabilità

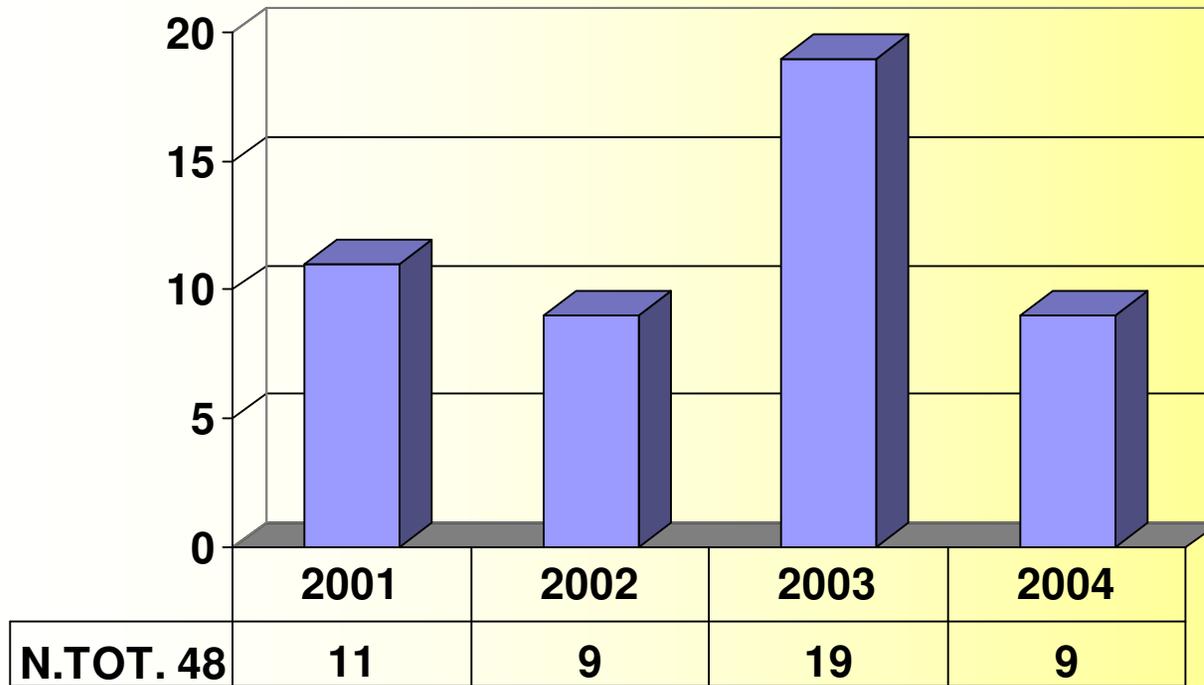
**COMPUTER
INFETTATI
IN "1 ORA"**



Fonte: McAfee AVERT

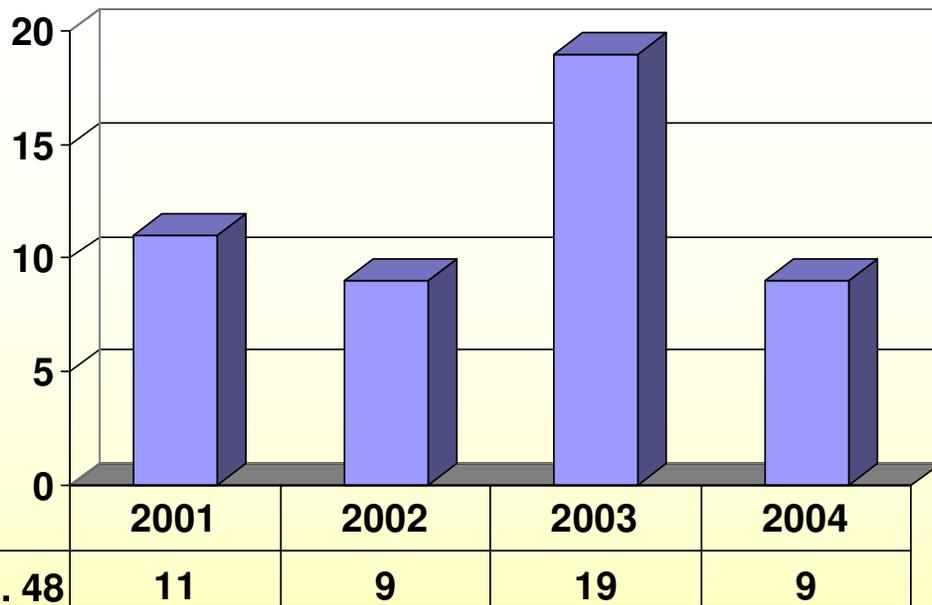


**IMPORTANTI
VULNERABILITA'
DEI S.O.
SEGNALATI DA
SECURITYNET®
DAL 2001 AL 2004**



AD APRILE 2004

LUGLIO 1	GENNAIO 1	MARZO 2	GENNAIO 1
FEBBRAIO 1	FEBBRAIO 1	APRILE 1	FEBBRAIO 2
MARZO 4	APRILE 1	LUGLIO 3	MARZO 2
APRILE 1	MAGGIO 1	AGOSTO 1	APRILE 4
MAGGIO 1	GIUGNO 2	SETTEMB. 1	
GIUGNO 2	LUGLIO 2	OTTOBRE 8	
DICEMBRE 2	SETTEMB. 1	NOVEMB. 3	



**IMPORTANTI
VULNERABILITA'
DEI S.O.
SEGNALATI DA
SECURITYNET®
DAL 2001 AL 2004**

AD APRILE 2004

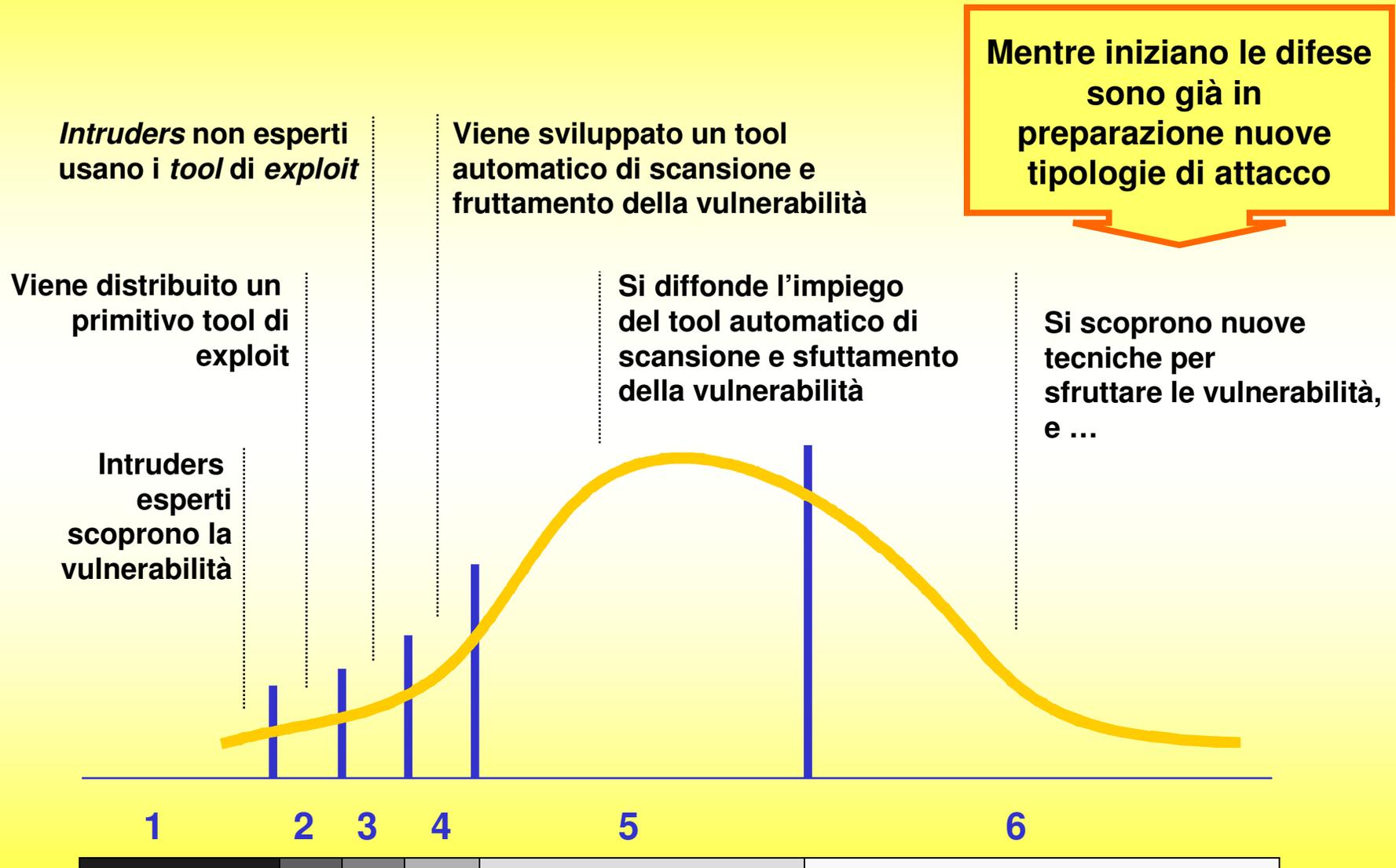
N.TOT. 48	11	9	19	9
------------------	-----------	----------	-----------	----------



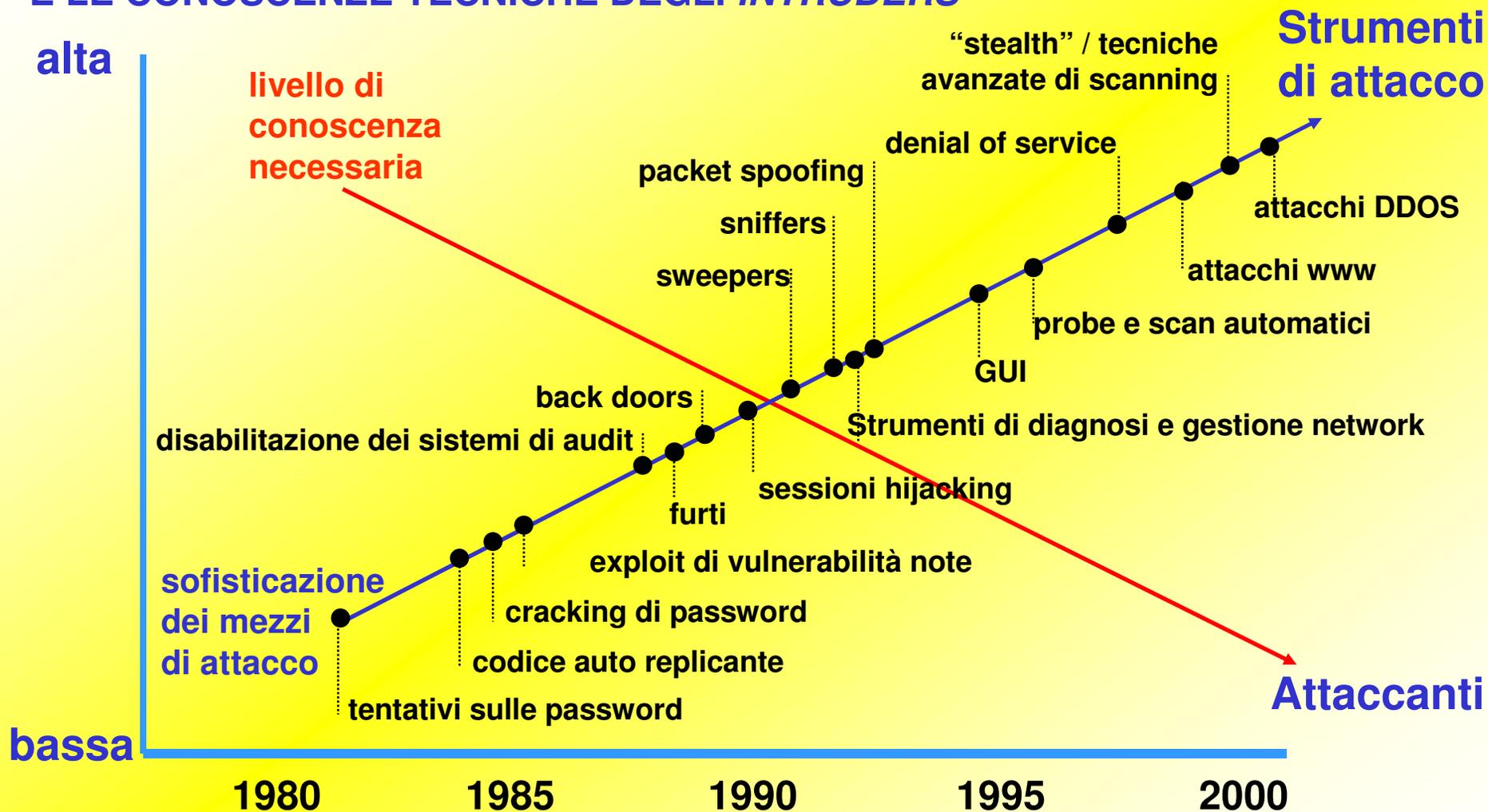
**MEDIA
GIORNI DELL'ANNO
E VULNERABILITA'
SEGNALATE
da SECURITYNET®**



CICLO DI SFRUTTAMENTO DI UNA VULNERABILITÀ DA PARTE DEGLI *INTRUDERS*



CONFRONTO TRA: LA SOFISTICAZIONE DEGLI STRUMENTI DI ATTACCO E LE CONOSCENZE TECNICHE DEGLI *INTRUDERS*





SINTESI DELLE ANALISI STORICHE NELLE AZIENDE ITALIANE

Da 3 anni non vengono scritti virus “tradizionali”

Si diffondono indipendentemente dai luoghi geografici

Lombardia, Lazio e Piemonte sono le regioni più colpite

L’ultimo quadrimestre dell’anno e maggio sono i periodi a maggior diffusione

Non c’è differenza tra categorie aziendali nella capacità di reagire

Dopo un periodo di flessione aumentano i virus circolanti

Da 3 anni le criticità provengono dalle e-mail, da Internet e da network worm

Virus camuffati da finte *patch* e *spyware*

Virus associati a spammer

Aumentano i virus (worm) che sfruttano le vulnerabilità per diffondersi

Aumenta la velocità con la quale i network worm si diffondono

Diminuisce il tempo tra la scoperta di una vulnerabilità e il relativo sfruttamento

DAI VIRUS AI NETWORK WORM

**Cosa accadrebbe
se nello stesso giorno
fosse scoperta e sfruttata
una nuova vulnerabilità ?**



USO DELLA POSTA ELETTRONICA

ASPETTI NORMATIVI,
RISCHI TECNICI,
PROTEZIONE ED USO SICURO

SECURITYNET
SERVIZIO ANTIVIRUS E PREVENZIONE COMPUTER CRIME

CC
Club sul Computer Crime

VIRUS, WORM E VULNERABILITÀ

Alcuni aspetti normativi e legali

Obblighi
Responsabilità
Sanzioni

Sono 3 le componenti indispensabili a garantire la protezione dei dati, la fiducia degli utenti e il patrimonio aziendale:

INTEGRITA'

la salvaguardia della esattezza dei dati, la difesa da manomissioni e da modifiche non autorizzate, il monitoraggio automatico degli accessi, ecc..

CONFIDENZIALITA' (riservatezza)

la protezione delle informazioni tramite l'accesso solo agli autorizzati, la protezione delle trasmissioni, il controllo accessi, ecc..

DISPONIBILITA'

la garanzia per gli utenti della fruibilità dei dati delle informazioni e dei servizi, evitando la perdita o riduzione dei dati o dei servizi

Sono i 3 PRINCIPI alla base delle nuove MISURE DI SICUREZZA, principi già presenti in STANDARD internazionali

ISO/IEC 17799:2000(E) - una parte di BS7799





Sono richiamati rispettivamente dalle Regole 16 e 20 del Codice in materia di protezione dei dati personali

ART. 615 QUINTES DEL CODICE PENALE

Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, ...

ART. 615 TER DEL CODICE PENALE

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito ...

IL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI



**INTRODUCE UN
NUOVO IMPORTANTE
DIRITTO**



**IL DIRITTO
ALLA PROTEZIONE
DEI DATI PERSONALI**

*“Chiunque
ha diritto alla protezione
dei dati che lo riguardano”*

**CONTIENE
LE PRESCRIZIONI
E LE REGOLE PER LA**



**SICUREZZA
DEI DATI
E DEI SISTEMI**

Art.1
(Diritto alla protezione dei dati personali)

**Chiunque ha diritto
alla protezione dei dati che lo riguardano**

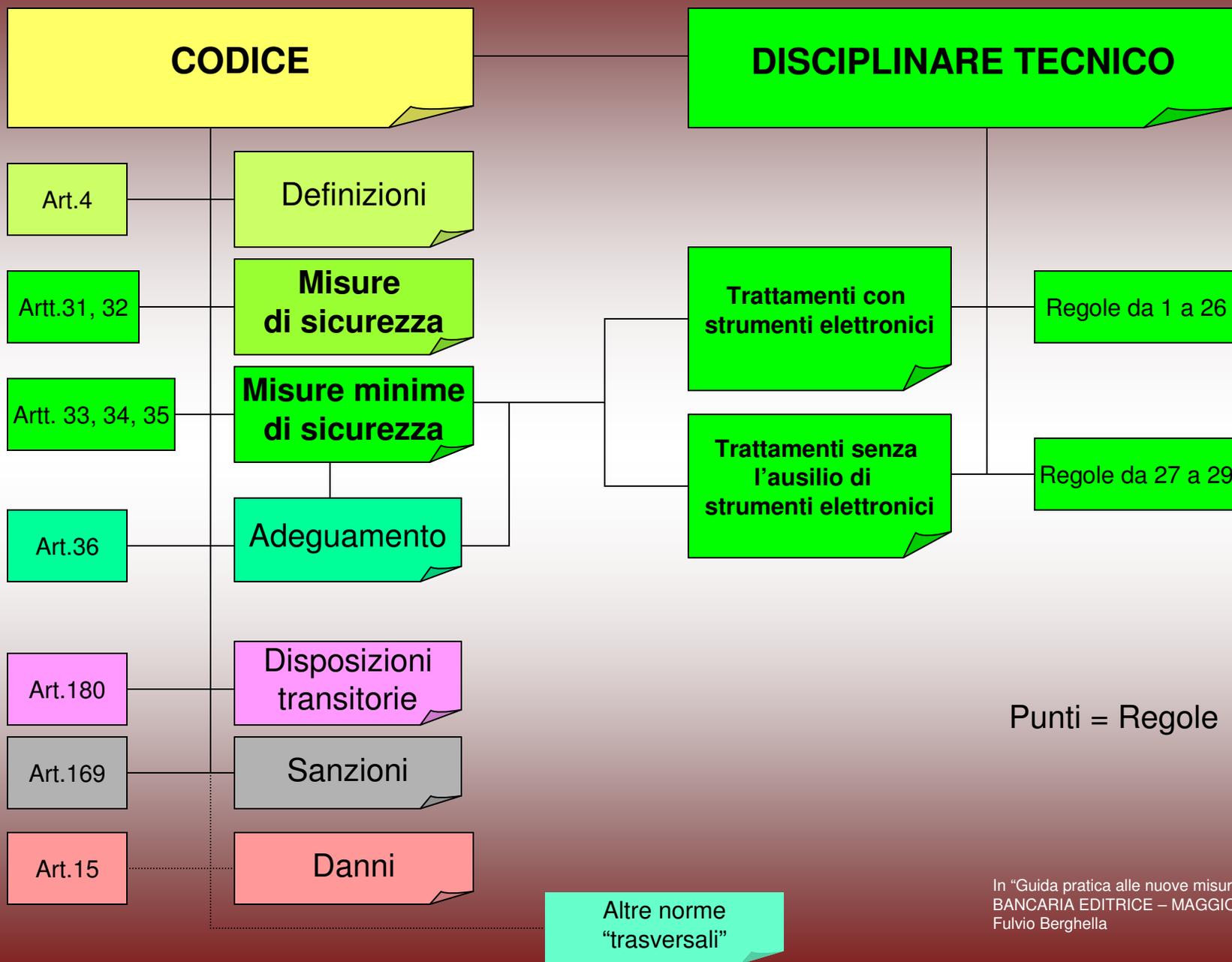
Riproduce il primo comma dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea (ora presente anche nell'articolo 50 del Progetto di Trattato che istituisce una Costituzione per l'Europa):

Protezione dei dati di carattere personale
**“Ogni individuo ha diritto
alla protezione dei dati di carattere personale che lo riguardano”**

“Il trasferimento di questa norma nel sistema italiano rende non più proponibili interpretazioni riduttive della protezione dei dati personali”

(Relazione del Garante del 28 aprile 2004)

ARTICOLAZIONE DELLE MISURE DI SICUREZZA



In "Guida pratica alle nuove misure di sicurezza"
BANCARIA EDITRICE – MAGGIOLI EDITORE ©
Fulvio Berghella

Art. 34 Trattamenti con strumenti elettronici

Il trattamento di dati personali effettuato con strumenti elettronici è consentito solo se sono adottate, nei modi previsti dal disciplinare tecnico contenuto nell'allegato B), le seguenti misure minime:

- a) ~~autenticazione informatica;~~
- b) adozione di procedure di gestione delle credenziali di autenticazione;
- c) utilizzazione di un sistema di autorizzazione;
- d) aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- e) protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- f) adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- g) tenuta di un aggiornato documento programmatico sulla sicurezza;
- h) adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

Altre misure di sicurezza.

Regole 15, 16, 17, 18 Disciplinare tecnico



Regola 16 e art.34, comma 1, lettera e)



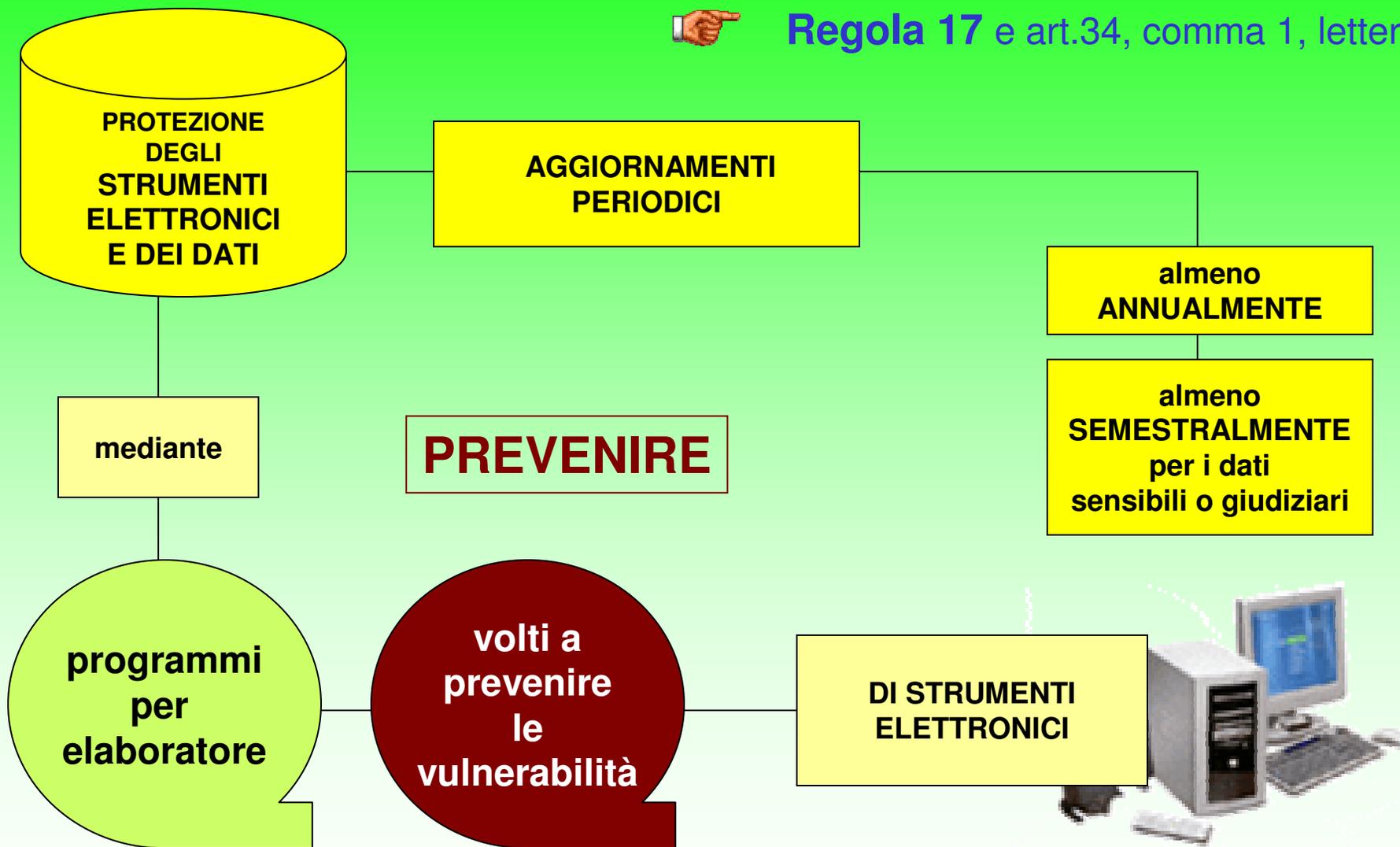
In "Guida pratica alle nuove misure di sicurezza"
BANCARIA EDITRICE – MAGGIOLI EDITORE ©
Fulvio Berghella

Altre misure di sicurezza.

Regole 15, 16, 17, 18 Disciplinare tecnico



Regola 17 e art.34, comma 1, lettera e)

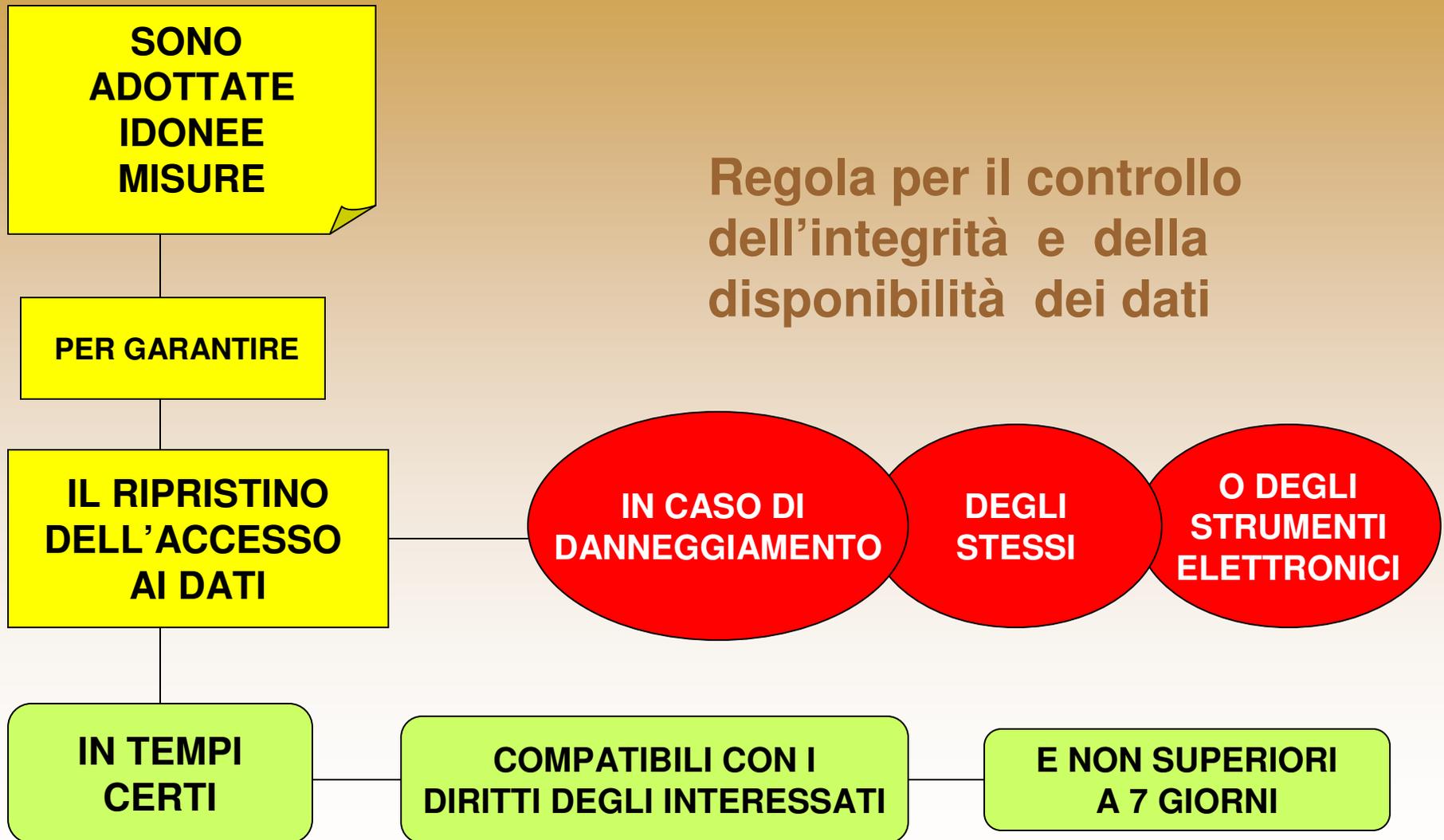


In "Guida pratica alle nuove misure di sicurezza"
BANCARIA EDITRICE – MAGGIOLI EDITORE ©
Fulvio Berghella

Ulteriori misure di sicurezza in caso di trattamento di dati sensibili o giudiziari. Regole 20, 21, 22, 23, 24 Disciplinare tecnico

 **Regola 23**

Regola per il controllo dell'integrità e della disponibilità dei dati



DOCUMENTO PROGRAMMATICO ANNUO SULLA SICUREZZA

Art.34, comma 1, lettera g)
“tenuta di un aggiornato documento programmatico sulla sicurezza”

REGOLE 19 E 26

Elenco dei trattamenti

Compiti e responsabilità

Analisi dei rischi

Integrità e disponibilità dati
Protezione aree e locali

Ripristino della disponibilità

Formazione per gli incaricati

Sicurezza e out sourcing

Salute e vita sessuale

Nell'ambito

Che inco

Per la pr
e a

Dopo distru

Su rischi, r

Criteri per

Criteri per

MISURE DI TUTELA E GARANZIA

Regola 26 Disciplinare tecnico

**Il titolare riferisce,
nella relazione
accompagnatoria
del bilancio d'esercizio,
se dovuta,
dell'avvenuta redazione
o aggiornamento
del documento
programmatico sulla sicurezza**

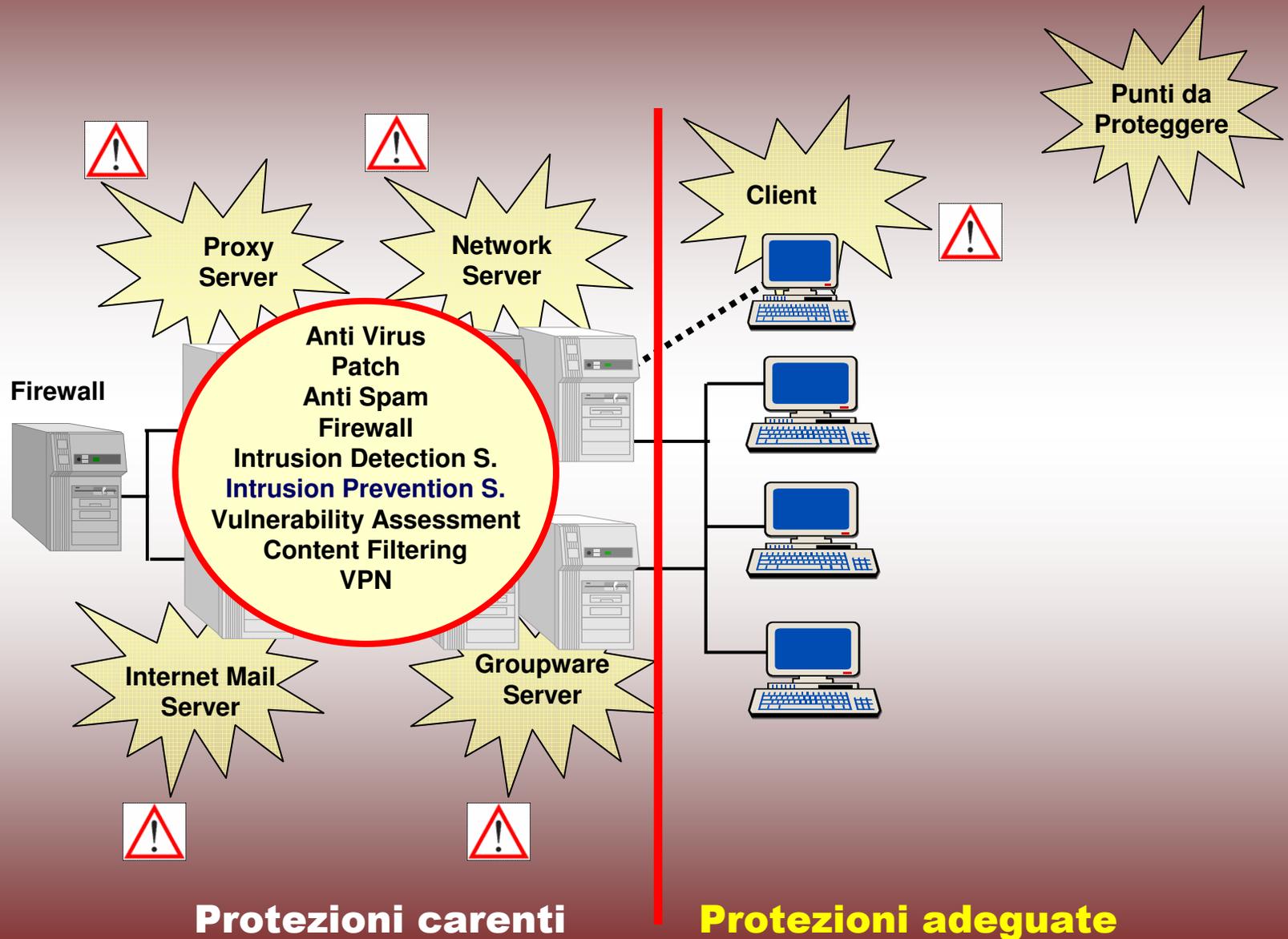
Cifratura

Dis

Disgiunzione

Altri dati

PUNTI CRITICI E VULNERABILI DI UNA RETE AZIENDALE, ATTACCABILI DA VIRUS, INTERNET WORM E CODICI MALIGNI



E-MAIL E-MAIL E-MAIL E-MAIL E-MAIL E-MAIL E-MAIL E-MAIL

FINE

**E ... GRAZIE
PER L'ATTENZIONE**

c.desantis @oasi-servizi.it