
**POLISH TELECOM
SECURITY INCIDENT RESPONSE TEAM**

Incident handling, statistics and procedures

Warsaw, May 2003

TABLE OF CONTENTS

I. INFORMATION ABOUT TP SECURITY INCIDENT RESPONSE TEAM	3
II. TP NETWORK	4
1. Technologies	4
2. Structure of the network	5
3. Access to the Internet	6
III. INCIDENT HANDLING	7
1. Incident classification	7
2. Incident handling - support computing	8
IV. STATISTICS OF INCIDENTS	13
1. Total number of registered incidents in 1997 - 2003	13
2. Total number of registered incidents - type of events (I-IV.2003)	14
3. Number attacks profile	15
4. Percent of recognised categories of the incidents	16
5. Complaints sender	17
6. Source of attack	18
V. INCIDENT HANDLING - INCIDENT RESPONSE	19
1. Cooperation	19
2. Incident response	20
3. Cooperation with Polish Police and Public Prosecutor	21
VI. CONCLUSION	23

INFORMATION ABOUT TP SECURITY INCIDENT RESPONSE TEAM

TP Security Incident Response Team*

- History of the team
 - ▶ **1997 - start**
 - ▶ **structure**
- Team's activities
 - ▶ **registration and classification of incidents**
 - ▶ **localisation of an intruder**
 - ▶ **incident response**
 - ▶ **analysis of new threats**
 - ▶ **others (conferences, working meetings, mass-media)**
- Basic rules of incidents handling
 - ▶ **gathering information from users, administrators, the police and other institutions about incidents concerning all addresses within Polish Telecom IP range**
 - ▶ **incidents reported by government institutions are handled first**

TECHNOLOGIES

VSAT

X.25, TCP/IP



Internet
TCP/IP



Frame Relay / ATM, X.25, TCP/IP

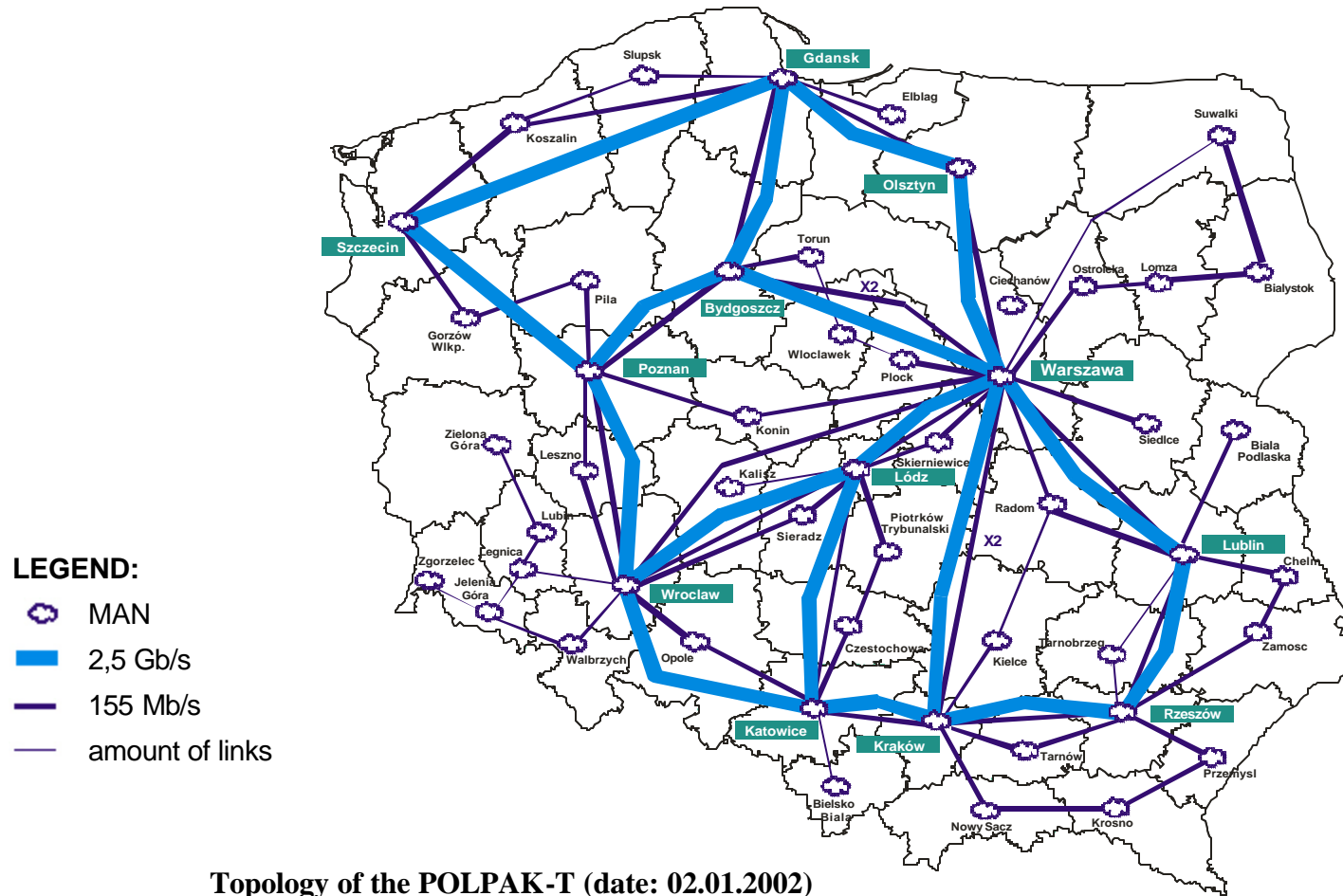


X.25, X.28, X.32

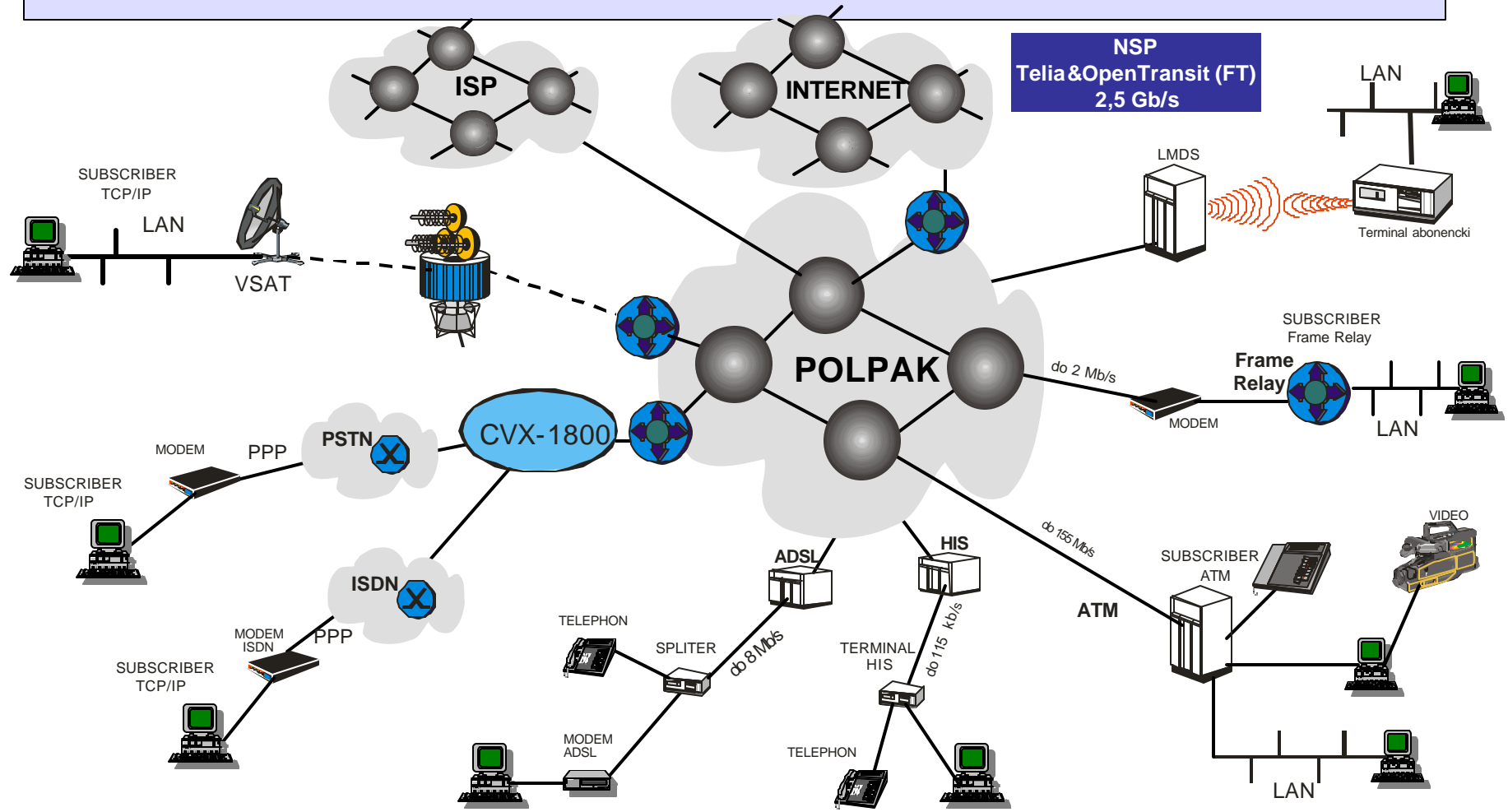


X.400, X.500, EDI

POLPAK NETWORK



ACCESS TO THE INTERNET



POLISH TELECOM CLASSIFICATION OF INCIDENTS

- H** - The most dangerous incidents (hacking, breaking in, modifying, deleting, stealing)
- P** – Type of events concerning hacking attempts (scan, probe)
- T** - Copyright and special incidents (requests of the Police, plagiarism, piracy)
- B** - Denial of service incidents (flood, DoS, DDoS, mailbombing)
- O** - Violation of the netiquette (offensive words, pornography)
- M** - Spam incidents (spam to advertise)
- R** - Spam-relay incidents (open relay, open proxy)*

STARTING THE 3rd QUARTER OF 2002 TP RESPONSE TEAM USE COMMON LANGUAGE CLASSIFICATION IN THEIR PROCEDURES

INCIDENT SERVICE SYSTEM (ISS)

Incident Service System (ISS):

- Is a database which allows gathering, registering and classifying of incidents
- Contains an advanced administration mechanisms and access control
- Automates incident handling process by:
 - ▶ **tracking incident handling process**
 - ▶ **quick access to stored incidents**
- Accelerates incident handling

ISS FUNCTION

Basic system function :

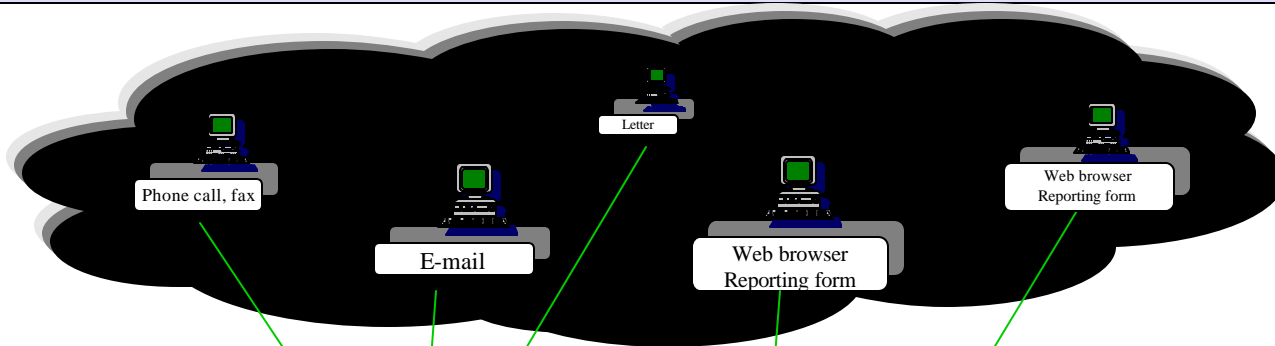
- incident importing from web site
- incident data inputting (from different sources)
- incident analysing
- incident searching
- printing warnings, reports, statistics
- sending reply
- intruder history

Other system function:

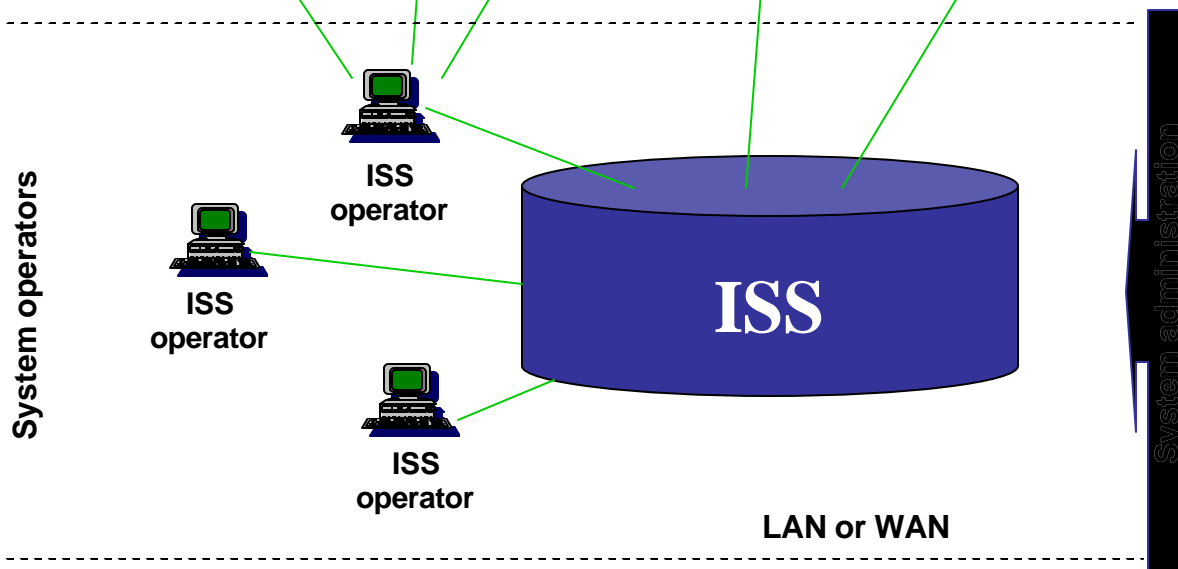
- contacts and information management
- incident handling process management
- task planning

ISS STRUCTURE DIAGRAM

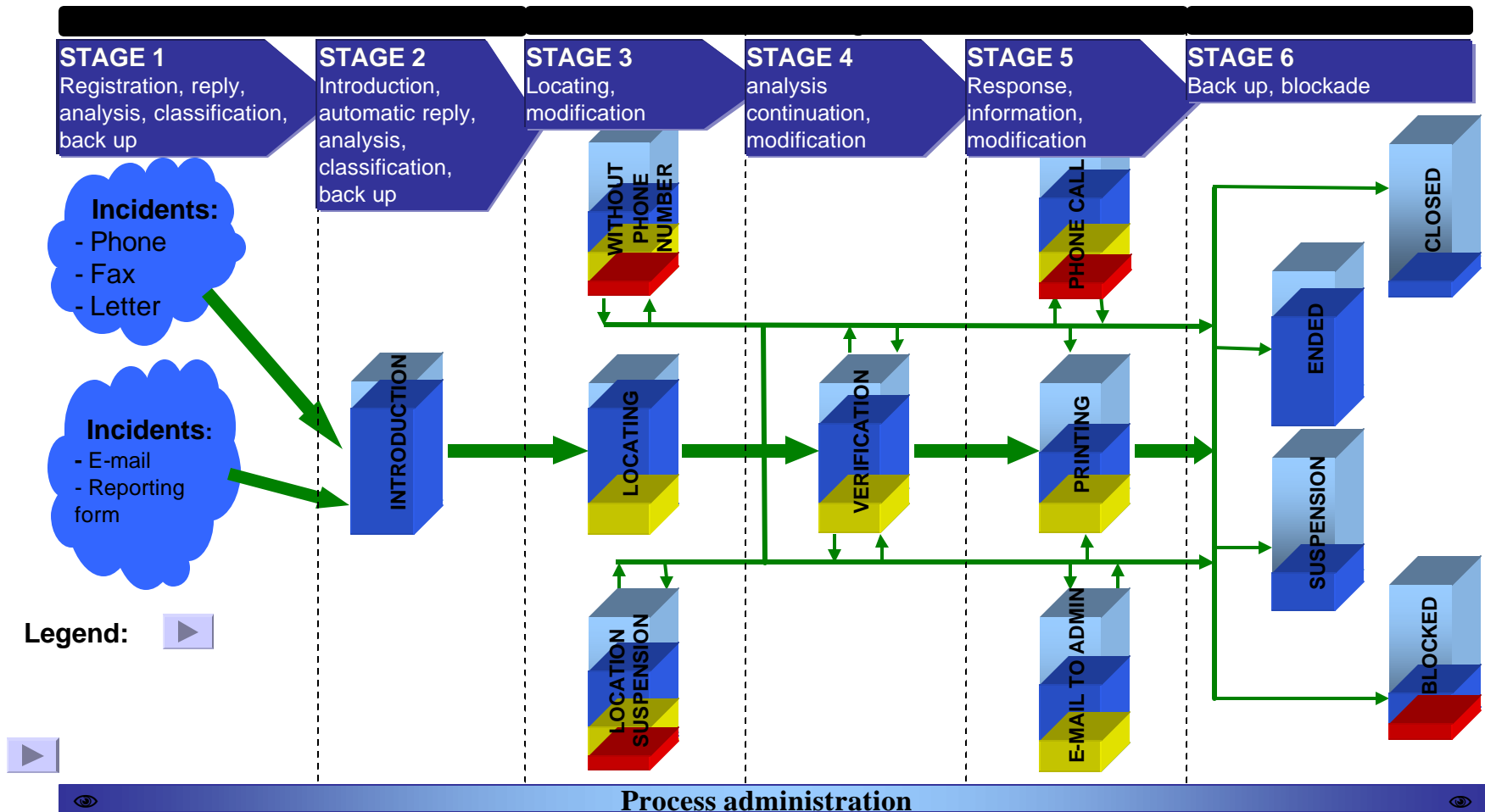
INCIDENTS



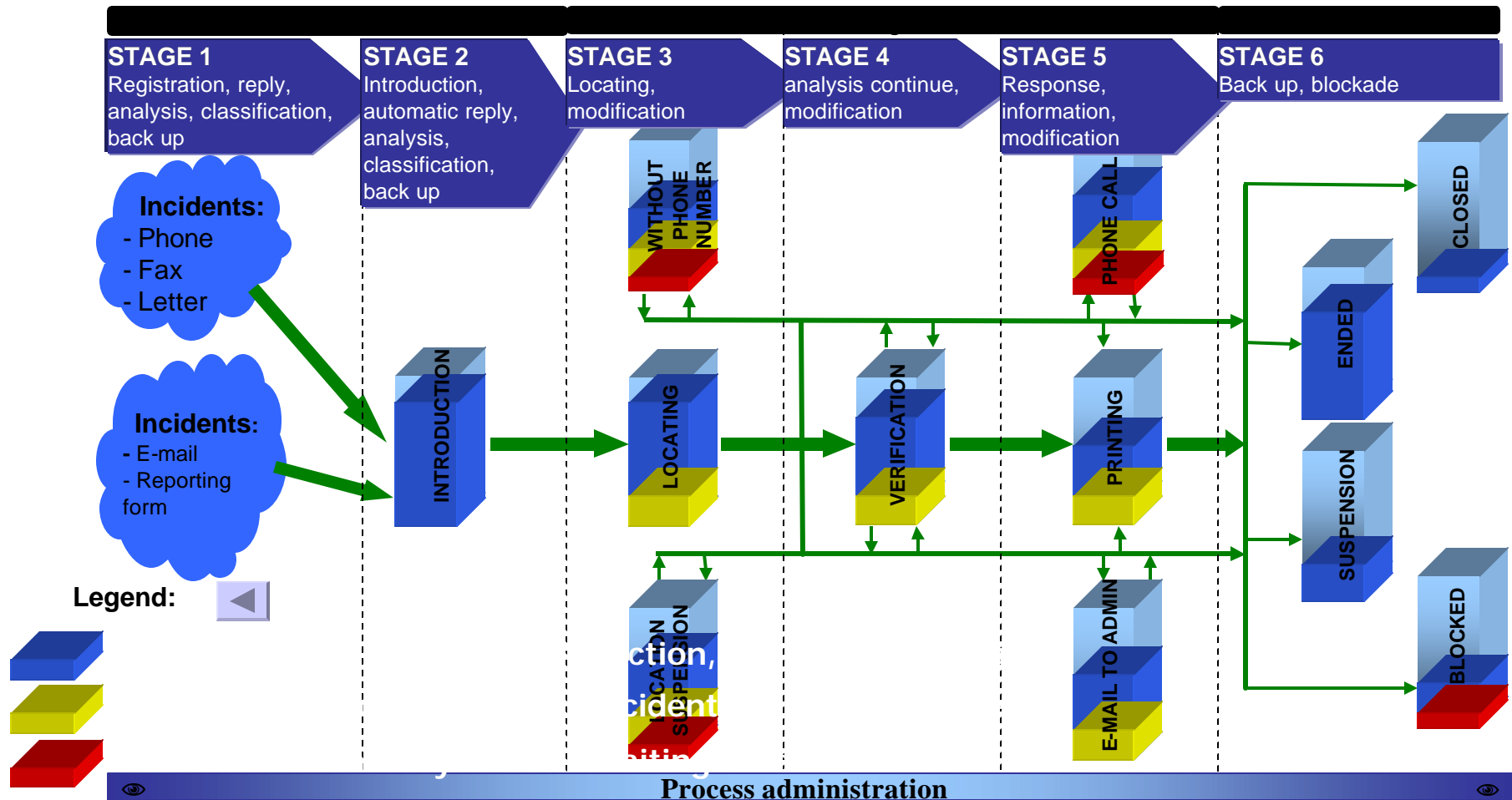
INCIDENT HANDLING



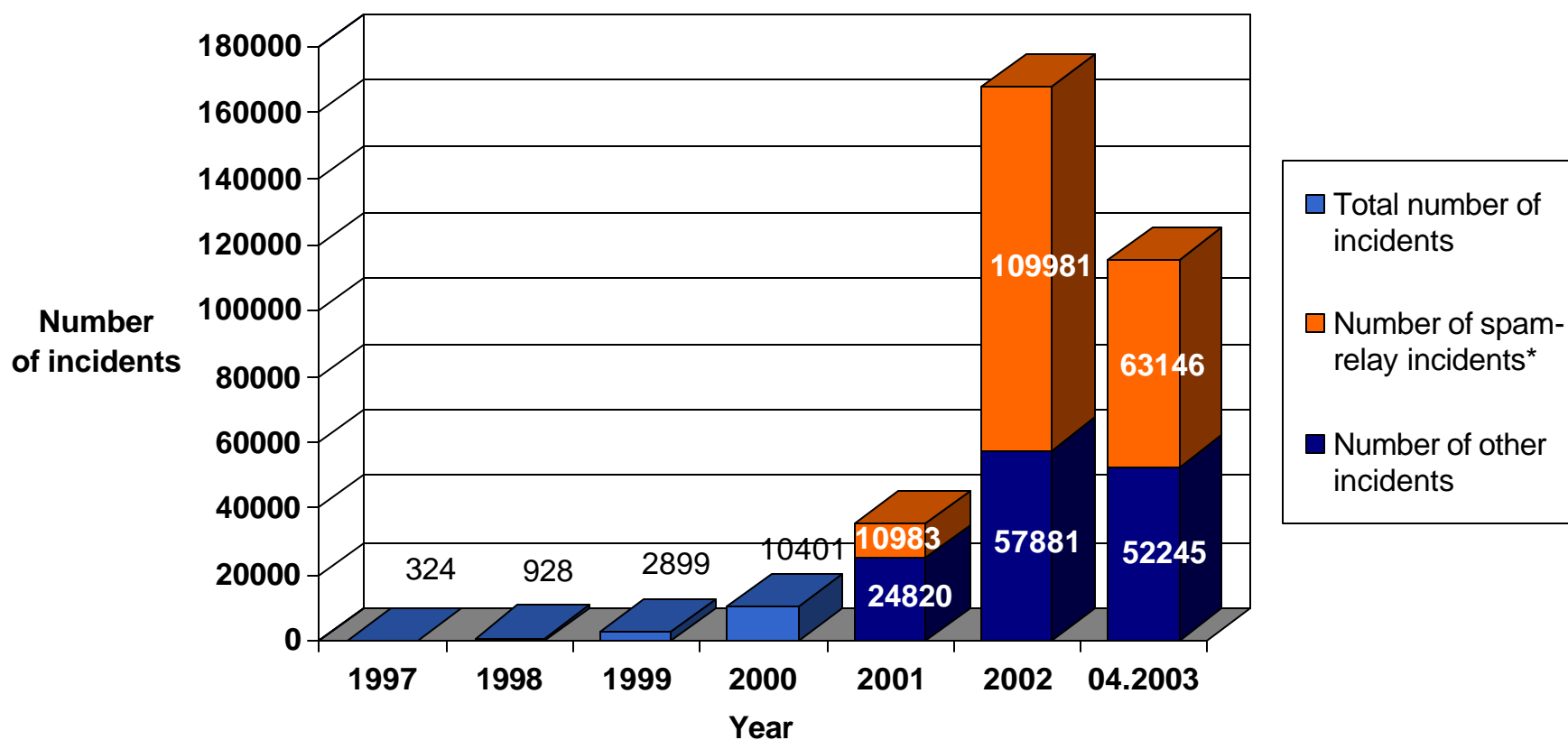
ISS INCIDENT HANDLING PROCESS DIAGRAM



ISS INCIDENT HANDLING PROCESS DIAGRAM

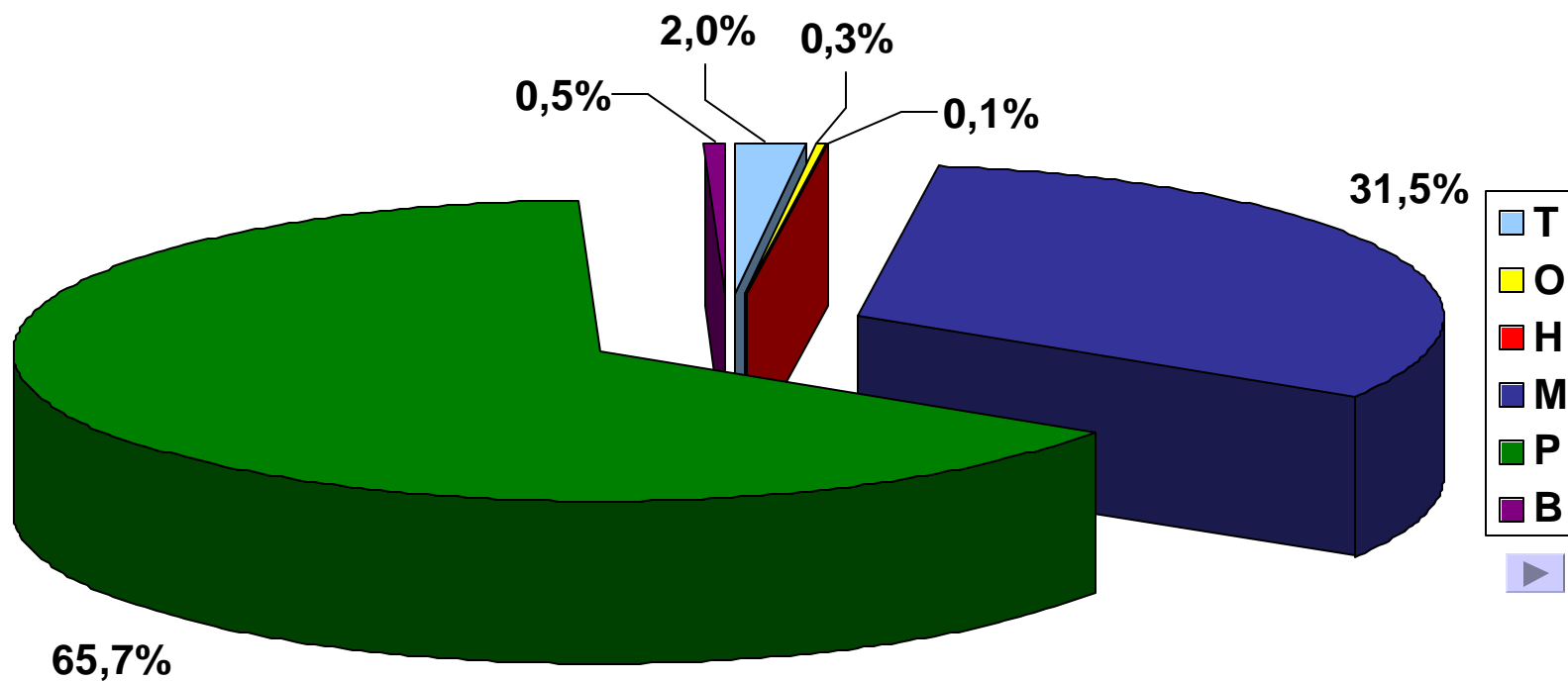


TOTAL NUMBER OF REGISTERED INCIDENTS IN 1997 - 04.2003



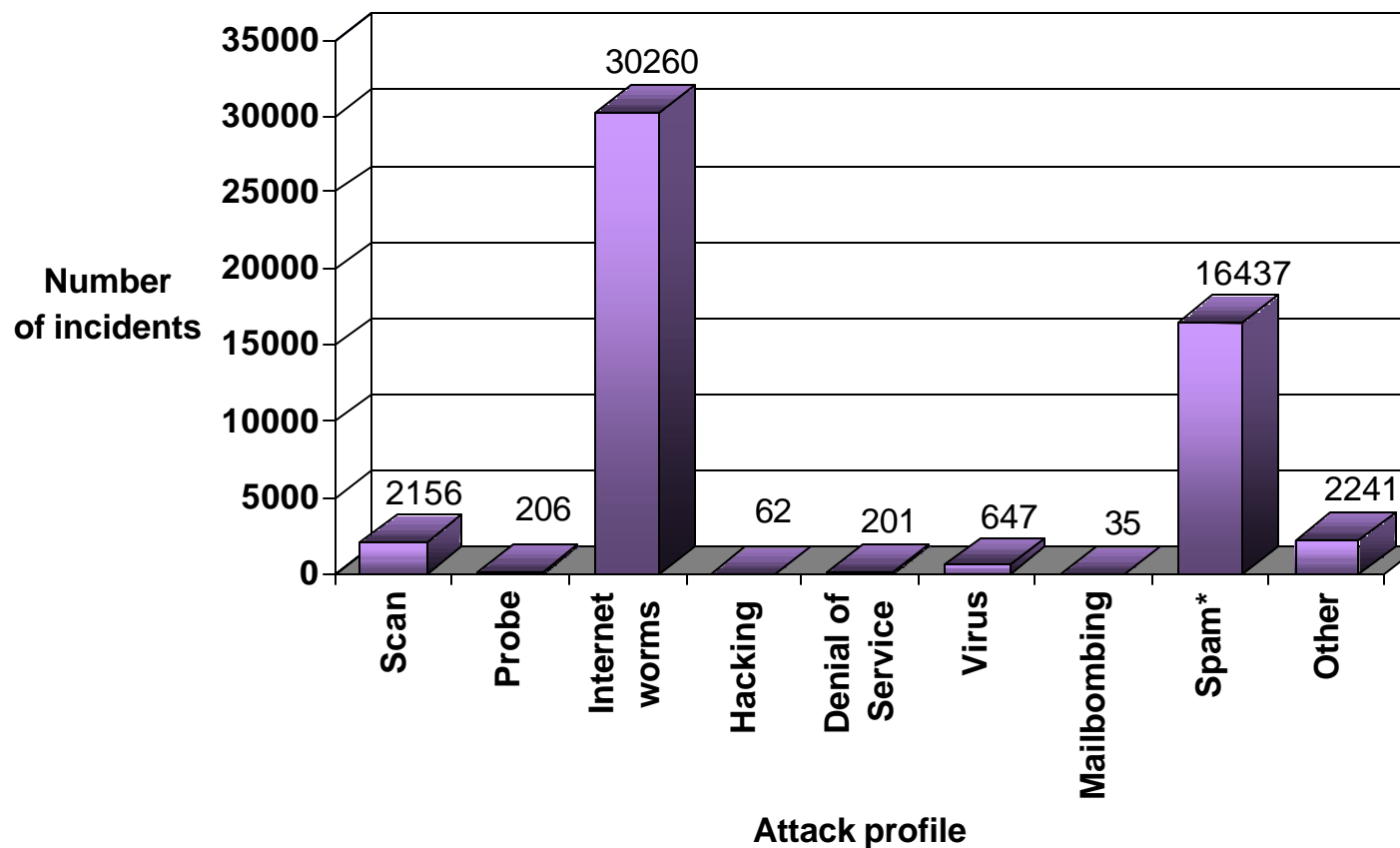
***/ Starting 2001 spam-relay events are not counted together with other incidents.**

NUMBER OF REGISTERED INCIDENTS - TYPE OF EVENTS (I-IV.2003)



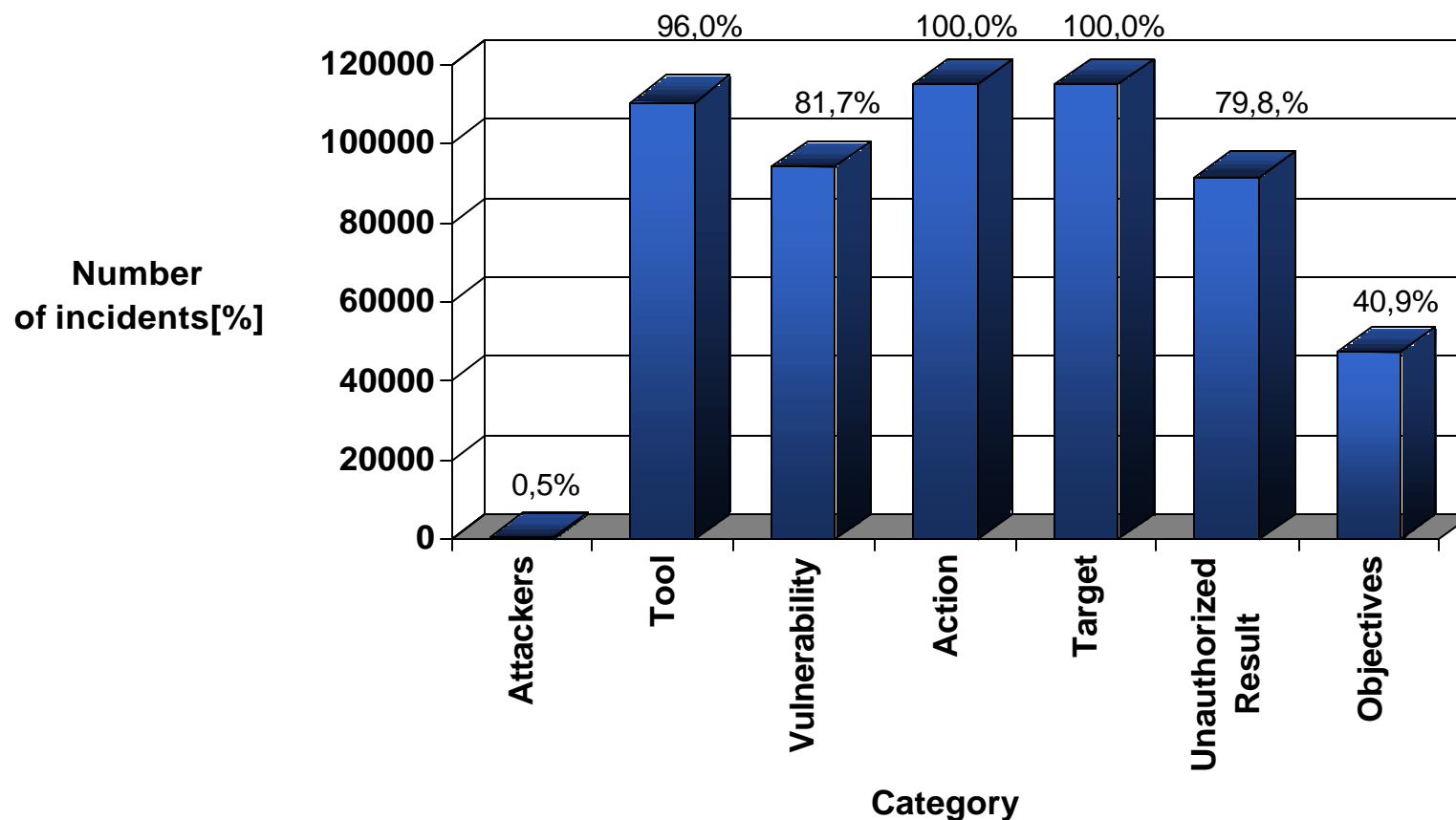
Spam-relay events were not included

PROFILE OF ATTACKS (I-IV.2003)

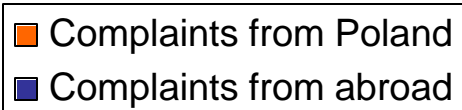
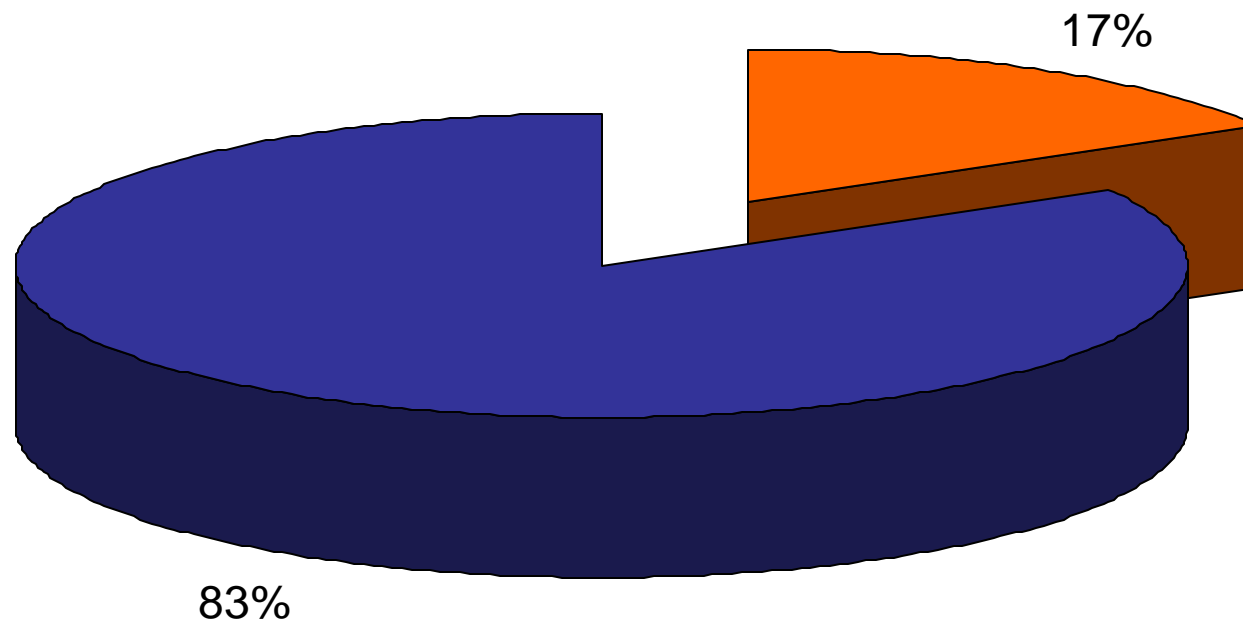


***/ Spam-relay events were not included**

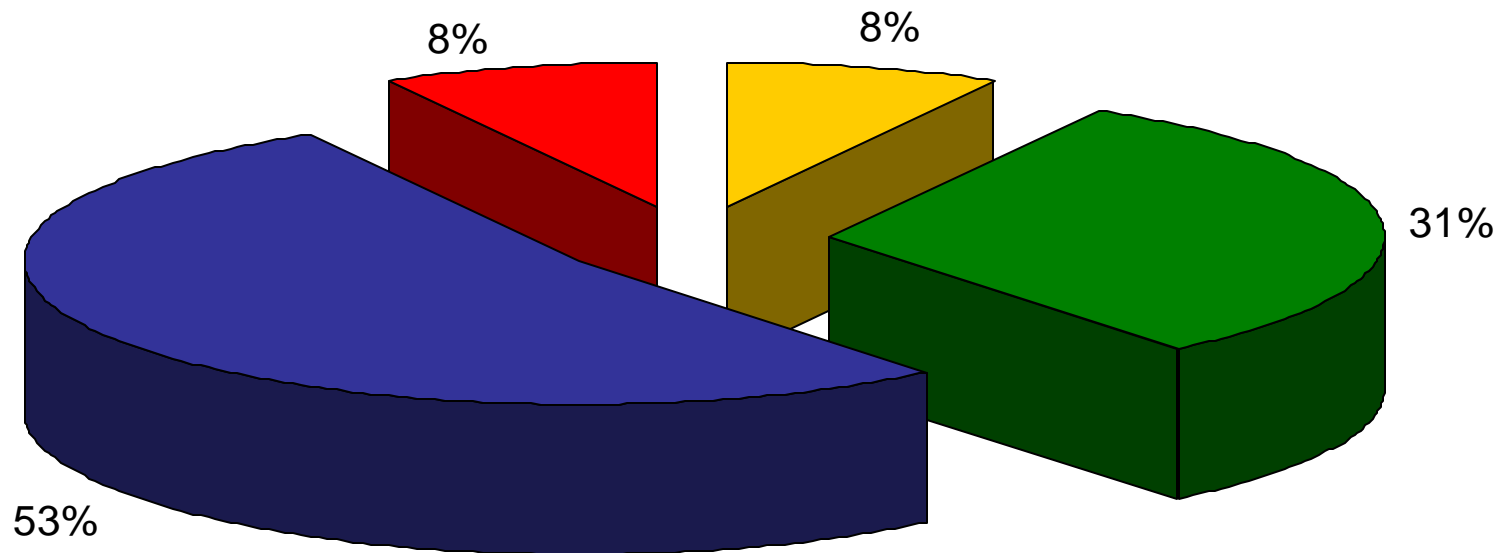
**PERCENTAGE OF RECOGNISED INCIDENTS CATEGORIES (I-IV.2003)
ACCORDING TO THE COMMON LANGUAGE CLASSIFICATION**



SOURCE OF COMPLAINTS (I-IV.2003)



SOURCE OF ATTACKS (I-IV.2003)



- Dial-up (0-20-21-22/24/30)
- Leased lines (FR)
- Home Internet Solution (HIS)
- Asynchronous Digital Subscriber Line (ADSL)

COOPERATION

- CERT Team (e.g. CERT Polska)
- The police
- Public Prosecutors
- Other government Institutions
- Other Polish ISPs

INCIDENT RESPONSE

I. Information/Warning

1. Phone



2. E-mail

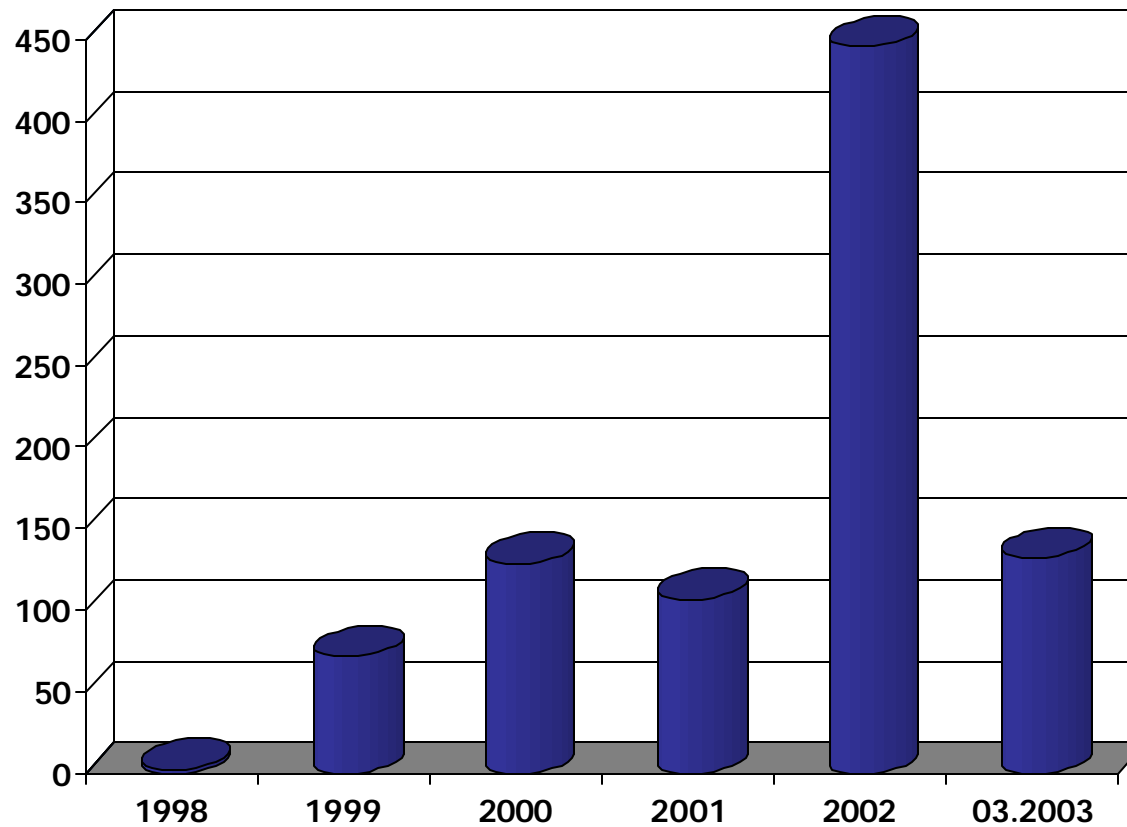


3. Letter



II. Blockade - discharge

NUMBER OF REQUESTS FROM POLISH POLICE AND PUBLIC PROSECUTOR



REGISTRATION OF DATA AND INFORMATION SENT THROUGH THE NETWORK

According to new regulations operators are obliged to enable selected government institution access to the following:

- **Data**
 - ▶ subscriber / user identification
 - ▶ location and identification connections between nodes in the network
 - ▶ type of connection and other data

- **Information sent through the network**

CONCLUSION

TP Security Incident Response Team*

- **Operate against network abuse incidents, the additional role is to prevent, educate and inform.** Team`s Web site, special line for victims, e-mails, warnings.
- **Trace kinds and ways of network abuse and adapt its procedures to current demands.** CERT Cooperation, Security sites in the internet.
- **Take active part in implementing standards of handle and incident classification.** Implementing the Common Language classification.
- **Cooperate with security institutions: the police, public prosecutors and network administrators.**

HOW TO CONTACT TP SECURITY INCIDENT RESPONSE TEAM - INCIDENT REPORTING

Incidents can be reported by:

- ***E-mail:***
 - abuse@telekomunikacja.pl
 - abuse@tpsa.pl
 - abuse@tpnet.pl

- ***Web site (On-line Form):*** http://www.tpnet.pl/eng_ver/abuse/php

- ***Address:***
 - TP S.A. - „POLPAK”
 - Network Security Department
 - ul. Nowogrodzka 47
 - 00-695 Warszawa
 - POLAND

- ***Phone:*** +48 /22/ 58-50-777

- ***Fax:*** +48 /22/ 824-14-52

ADDRESS SHEET

PRESENTATION DEVELOPED BY:

Division:	TP SA - „POLPAK”
Department:	Network Security
Phone #:	+48 /22/ 58 50 777
E-mail:	abuse@telekomunikacja.pl
Web site:	http://www.tpnet.pl/eng_ver/abuse/php