UNITED
NATIONS

E

Economic and Social
Council

Distr.
GENERAL

CES/AC.71/2001/17 (SUM)
5 December 2000

Original: ENGLISH

STATISTICAL COMMISSION and ECONOMIC COMMISSION FOR EUROPE

COMMISSION OF THE EUROPEAN COMMUNITIES (EUROSTAT)

CONFERENCE OF EUROPEAN STATISTICIANS

Joint ECE/Eurostat Meeting on the Management of Statistical Information Technology
(Geneva, Switzerland, 14-16 February 2001)

Topic (ii): Challenges and opportunities for statistical offices working in a network environment

THE PROBLEMS CONNECTED WITH SECURITY OF DATA TRANSFER VIA NETWORK AND THE SOLUTIONS IMPLEMENTED IN THE CSO OF POLAND

Submitted by Polish Central Statistical Office [1]

CONTRIBUTED PAPER

SUMMARY

1. The security of the collected, processed and disseminated statistical information is treated very carefully by everyone in the statistical office. It is undoubtedly true that it is not possible to construct a system with unbreakable security in all areas. In practice, we find that some degree of risk must be accepted, because, as security systems are becoming more and more sophisticated, so are hacking techniques. In order to effectively protect confidential information, it is necessary to find possible weak areas, which might become a cause of loss of confidentiality, integrity or availability of that information. For each area at risk, it is necessary to determine all realistically possible ways in which security can be broken, and develop methods to prevent such events. It can be helpful to outsource such services to companies specialised in implementing data security systems.

[1] Prepared by Halina Agnieszka Stegawska.

2. The term “security policy" covers all tasks of management, administration, technical personnel, users and all other members of the organization for maintaining the necessary level of security of the statistical information system. This safety level is illustrated by the number of security features used. It serves to control access to resources (equipment, software, documentation, raw data), data confidentiality, authentication and data integrity.

3. Possible problems in the breach of security of data in computer networks can be divided into three main categories:

- intentional breach of security – the theft of an inscription key, or tapping of a network connection;
- unauthorized data access - by logging in using a stolen or guessed password;
- denial of service – due to the breach of security system, users can not use a given or all services of the network or server.

4. The basic techniques already in use or planned to be used to ensure network security are: identification (users are identified through a password), authentication (verification of user’s identity), authorization and access control (assigning access rights to a user), protecting the confidentiality of information, data integrity (ensuring that the document was not modified during transfer) and digital signatures.

5. Another problem is secure Internet access, as well as access from Internet to the corporate WAN-CSO network. All data processing resources inside CSO’s Intranet are behind the firewall, not accessible to external users. Only www servers with public databases outside the firewall are accessible via Internet. Users working in regional statistical offices and in CSO LAN have access to the Internet only through a central firewall system. Use of the Internet services requires user authentication, and authorization for services such as email, www, telnet, and ftp. The system firewall is assisted by two additional routers, which make any hacking attempt into the system much harder.

6. A data security system needs to be constantly updated to make use of new techniques that ensure a higher level of safety. With this under consideration, CSO is working on improvements in the areas of:

- determining weak points in the currently used firewall system, it’s modifications, or possible replacement;
- changing the operating system to WINDOWS 2000 Servers and Windows 2000 PC;
- replacement of part of the equipment working in Local Area Networks and CSO Corporate Network with equipment of higher security level- e.g. Switch L3, new generations of the routers;
- implementation of the cryptography of data on the server and WAN levels;
- updates to the "Rules and Regulations for the Users of Computer Networks" and their implementations.