PROTECTION AND SYSTEM MAINTENANCE COMPUTER AND COMUNICATION SYSTEM OF EXECUTIVE COUNCIL OF AUTONOMOUS PROVINCE OF VOJVODINA

Milan Paroški[1],
Nenad Petrović, Rade Ćirić[2]
[1]Provincial Authorities Administrative and Technical Services
[2]Provincial Secretariat for Science and Technological Development

I. INTRODUCTION

During 2007 and 2008 is implemented LAN and WAN computer network Executive Council and the Assembly of the Autonomous Province of Vojvodina, as well as installation and pick up a range of services and application programs in the framework of the implementation of the program eVojvodina and action plan from the strategy of e-Government provincial authorities. A large number of applications and users and the importance of using the service is requested the necessity of protection and system maintenance computer-communication system IV AP Vojvodina.

II. REALIZATION

1. Physical protection equipment

a. No access to unauthorized persons communication equipments, setting distribution computer wardrobes with key and lock communication room.
b. Set up video surveillance with cameras (250 cameras, 20 servers, software for surveillance, management and control...) For security and load flow data, complete network performance is done in parallel with the existing computer network.
c. During the realization of the project system for registration and records of working time and control access to employees in the Assembly and Executive larger APV, which should provide:
    i. registration of all entries and exits of employees in the Assembly and the Executive Council of APV and recording work time,
    ii. registration of all entries and exits of vehicles in the Assembly and the Executive Council of APV,
    iii. access control and record entries and exits of employees in the protected premises,
    iv. defined zone forbidden access (ID cards for guests and contractors).

2. Protection of telecomunication rooms

a. Conducted cooling room.
b. Used inflammable materials.
c. Established fire alarm.

3. Equipment power supply

a. UPS conducted using diesel aggregates.
b. Set UPS (uninterrupted power supply) to the remote diagnosis and automatic reporting via e-mail.

4. Protection of computer equipment

a. Realized antivirus and antispam protection - provided the security of all computers in the local network of all malicious applications and viruses that could damage or harm the functioning of the workstations, servers and the local network as a whole. Antispam does not allow undesired e-mails to pass to clients on base assigned criteria.
b. WSUS (Windows Server Update Services) - enabled update all Windows operating systems through server installed WSUS service. WSUS Server download all Microsoft updates and distributes the client workstations. In this way keeps the bandwidth Internet link for client workstations update draw only from the server that is local and on the other hand over security update keeps the local network safe and eliminate the potential problems caused by failure of the operating system.
c. Set firewall (basic and advanced access control lists for access-pass control, translation and mapping port, authentication and authorization through RADIUS protocol, the warning-alerts).

5. *Software for monitoring and control system and equipment*

a. LMS - CISCOWORKS installed software configuration management and the entire active network equipment and analysis of network traffic.
b. Using software to analyze the security hole for web sites and provincial authorities in the web hosting server IV APV (trial software).
c. Installed and configured software for remote computer inventory - IBM Tivoli Provisioning Manager Express for Inventory 4.1.1 in order to:
    i. Effective collection, storage and maintenance of information about the software and hardware on PCs and servers, including Windows security patch-es.
    ii. Accurate insight into the number of licenses required for each installed software on all computers user to easily access full license and held true situation.
d. Installed software for remote management and administration of Windows system - Dameware NT Utilities version 6.7.0.8 to:
    i. use of administrative tools, which facilitates and promotes the administration workstations and servers in the network.
    ii. remote review of printers, registry, sevices/ devices, system tools, TCP Utilities, user accounts, Event Log-s etc.

6. Redundancy

a. Redundancy computer-comunication infrastructure :
    i. (backup) central switch CISCO 4506 and twenty GBIC-s.

ii. Backup of every diferent model of hundred switch-es in total.
iii. All optical connections to the distribution cabinet (vertical backbone) doubled.

b. The room in which the Executive Council held the session and the session working bodies and commissions covered by cable and wireless connection.

7. BACKUP

a. In progress is realization of backup link for access to internet over another internet provider.
b. Installed software for backing up data and operating systems on servers – Symantec Backupexec. This is enabled:
   i. centralized and automated storage to copy data on a separate disk device and directly to the strip.
   ii. quick recovery to the state system for any moment that can happen as a result of damage or delete data.
   iii. constant protection of the mail box all users account in the domain and SQL database.
   iv. software offers automatic recovery of server software on new hardware, without manual installation of the Windows operating system, backup agent and applications. Using tape storage devices and set bar is done daily incremental backup and weekly full backup.

8. Automation support users

Installed software Service desk to help users and automation support to users and local and remote administrator's subsystems for:

i. receiving a user request,
ii. tracking user requests,
iii. create and update the database of knowledge,
iv. various types of reports and insight into the engagement of technicians, the status of requests, etc,
v. monitoring contracts and so on.

9. Outsourcing support

a. In progress is procedure of Microsoft prodacts legalization.
b. In progress is implementation of premier support services, which administers the computer-communication infrastructure and the Executive Council of APV, receive appropriate professional and technical assistance in order to prevent and quickly eliminate incidentnih situation. Also, a series of training within the services of an administrator will be constantly upgraded.

10. Authorization and sertification

a. Realized Domain user authorization.
b. To all user computers removed administrative privileges and disabled installation of new software and hardware.
c. Elevated CA certificate and only authorized portable allowed computers to connect (wireless) network in the Executive Council and the Assembly of Vojvodina.

d. In the progress implementation of the pilot project to establish an internal public key infrastructure (PKI system) in the information system of provincial administration, training users, configuration certified body - CA (Certification Authority) server and services (Certificate Services) in the intranet environment, and the use of digital certificates, the introduction of hybrid smart card and PKI USB token in practice. Goal: training for a specific application of digital signature in the business environment in accordance with applicable law and laws

11. Reporting

a. MRTG (Multi Router Traffic Grapher) - a tool for tracking load network links with live presentation of the network traffic. Use it for tracking input and output bandwidth in bits/sec, connections per second, the total number of simultaneous sessions.
b. ISA reports-one of the functionality of ISA Server 2004 and the possibility to get a report on the activities and flow on the network during the previous day, or some other set time. Report comes in the mail automatically generates and sends to system administrators. The report brings us a number of useful information divided into several groups:
   i. Summary report (by protocol, top users, top web sites, cache performances)
   ii. Web users (top browsers, object types, operating systems)
   iii. Security (Authorization failures, dropped packets).

III. FURTHER ACTIVITIES

In order to maintain the current state and permanent improvement and development it is necessary to:

1. always inform users and create awareness about the risks and safe behavior,
2. educate employees about safety risks
3. ensure that each account has a password, and use all the rules regarding passwords,
4. check date antivirus protection,
5. periodically evaluate the security situation and check the computer network,
6. regularly check with the manufacturer if they are published new patch and apply patches and improvements,
7. use strong encrypt techniques and regularly check integrity software
8. secure programming techniques to use when writing software,
9. be careful when using and configuring network,
10. regularly checked on-line archive on the topic of security,
11. keep track of user accounts and system events (auditing), and regularly check the system log files,
12. when employees leave the company immediately terminate rights of access network.
13. do not run any unnecessary network service.

This is only part of that constantly need to monitor and promote in accordance with the development of hardware and software systems in order to protect security of eGovernment security system.

Novi Sad, 20.12.2008.

Prepared: Milan Paroški MSEE, Nenad Petrović BSEE, Rade Ćirić PhD

Information about the first author: Milan PAROŠKI,
Assistant Director of Provincial Authorities Administrative and Technical Services

Email : milan.paroski@vojvodina.gov.rs