IPTV SOLUTION

DAAC SYSTEM
INTEGRATOR

DAAC System Integrator has implemented IPTV services platform for the biggest Internet provider and telecom operator in Moldova – Moldtelecom. As a result of the project, Moldtelecom released digital TV service based on IP technology. Launch of IPTV remarked enhancement of Moldtelecom services and allowed the company to meet Clients' demand, offering its subscribers advanced television services at reasonable prices.

Moreover, in 2016 DAAC System Integrator has extended the initial IPTV platform of Moldtelecom by deploying multiscreen solution, which allowed the telecom operator to introduce multiscreen service, reaching new customers through its mobile offering. The introduced service delivers unified and intuitive entertainment experience to Moldtelecom subscribers, enabling them accessing live content through the application, and managing and watching network DVR recordings and video on demand.

BENEFICIARIES OF THE SERVICE

- Moldtelecom

KEY INDICATORS

- 140+ TV Channels
- High Definition
- 100k+ TV Endpoints
- Interactive Functionality
- Multiscreen delivery

ADVANTAGES OF THE SERVICE

- Digital image and sound quality
- Electronic program guide (EPG)
- Time shifting: pause and repeat functions
- Possibility to record favorite TV programs
- Composition of list of favorite TV channels
- Parental control
- Multi language subtitles and audio tracks
- Multi language interface (menu): English, Romanian, Russian
- Possibility to set notifications
- TV archive

DESCRIPTION OF THE SOLUTION

IPTV solution of Moldetelecom consist of 4 main parts:

- Content origination
- Content processing
- Content recording
- Streaming

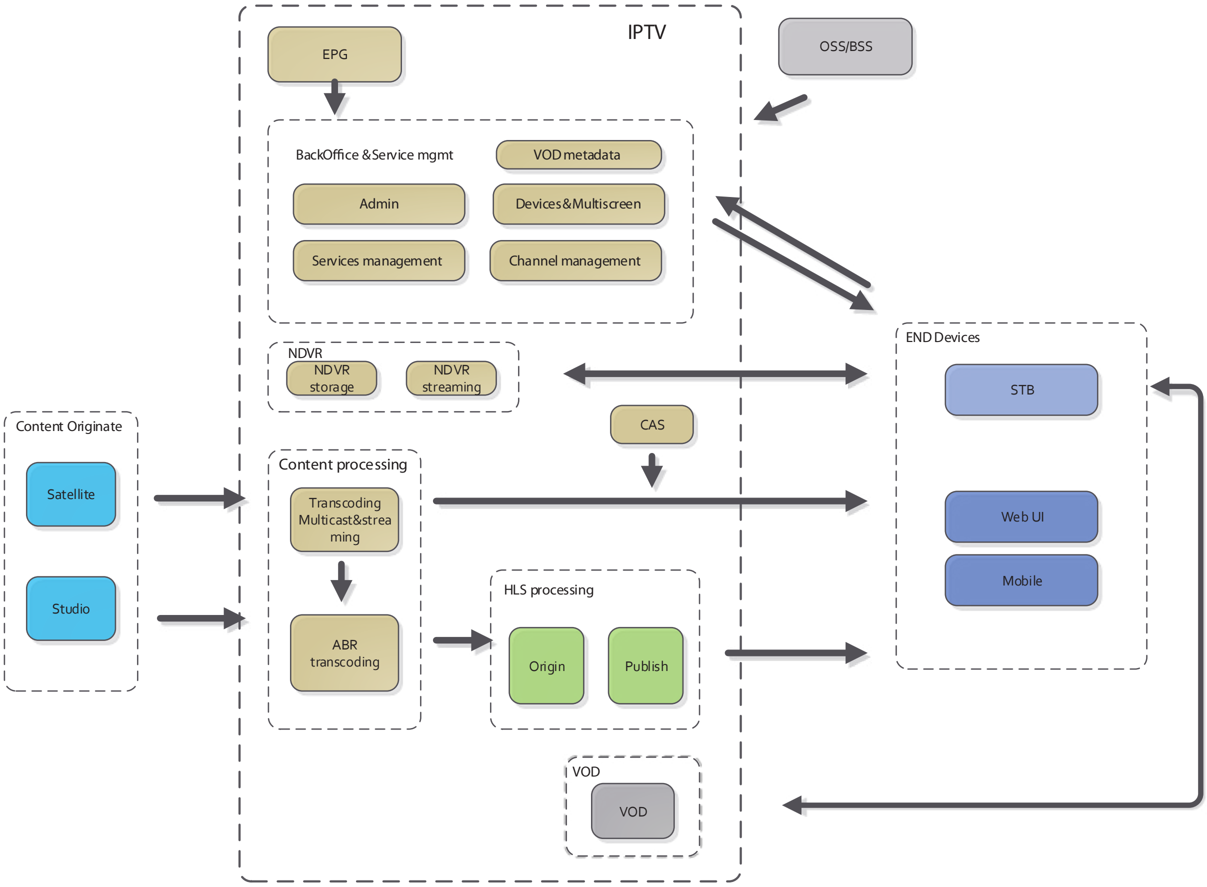
Content origination implies installation of satellite antennas on Moldtelecom site and connection of studios via Fiber links. Satellites are equipped with matrixes, which pass signals to receivers. Receivers get signals via RF interfaces, descramble different formats of signals and produce IP on output.

After a signal has been transformed in “pure” IP, it has to be processed. In case of MTC this implies transcoding MPEG2 to MPEG4. Moreover, the processing stage requires stabilization of bitrate and audio alignment. Transcoders produce multicast groups as an output, which could be used for end-devices such as STBs. Content can be secured here by CAS system.

At this point the system starts to record the necessary channels and programs for future use by NDVR, PLTV, Restart, CUTV.

HLS content creation starts at this stage too. Multicast groups, created by transcoders, are listened by HLS transcoding part, which creates ABR content for http streaming. HLS transcoder extracts video and audio content from multicast traffic for particular channels, chunks it and creates HLS profiles for publishing on origin servers. Origin servers process end-devices requests, providing HLS links for end-device APP.

End device applications (including mobile devices) are registered on middleware system part. All services, channel packages and additional options are controlled by middleware. Moreover, middleware keeps VOD metadata, where VOD service provides end-device with URL, addressing it straight to VOD provider of video servers.



DAAC System Integrator has successfully implemented the project of complex automatization of the call center of the National Telecom Operator of the Republic of Moldova – Moldtelecom. The list of technical requirements of the project included more than 200 components.

DAAC System Integrator managed to meet those requirements elaborating unique solution, based on software developed by NAUMEN and integrated with more than 10 information systems. This solution allowed automation of more than 200 work places and supports the operation of up to 1400 joint lines. New functionality of the system enlarged the possibilities of interaction with clients. Thus, now it became possible to process requests through different channels: voice calls, e-mail, chat, SMS, Skype, calls from the webpage.

OBJECTIVES OF THE PROJECT

The implemented solution had to possess parameters that ensure its consistent operation in the network and interaction with Moldtelecom IT infrastructure. The project implied integration of the call center with billing systems for authorization and pricing of paid services. At the same time, it was required to ensure full localization of software interface of the new solution.

Switching part of the component had to provide the possibility to organize 20 PRI E1 voice streams with the support of SS7 signaling, maintenance of 500 simultaneous connections in SIP format and creation of 1200 IVR channels. Moreover, new platform had to enable interaction with clients via diverse channels (email, SMS, chat, voice calls and other channels) and carrying out “tele voting”.

DESCRIPTION OF THE PROJECT

The proposed solution is based on NAUMEN platform, which is used in more than 50 call centers of telecommunication companies. DAAC System Integrator and NAUMEN elaborated the systems project, which implies Dell server equipment, AudioCodes Mediant 2000 media gateways, soft switch Fastwire OpenCA and Naumen software: Contact Center, DNS, Network Manager.

KEY FEATURES

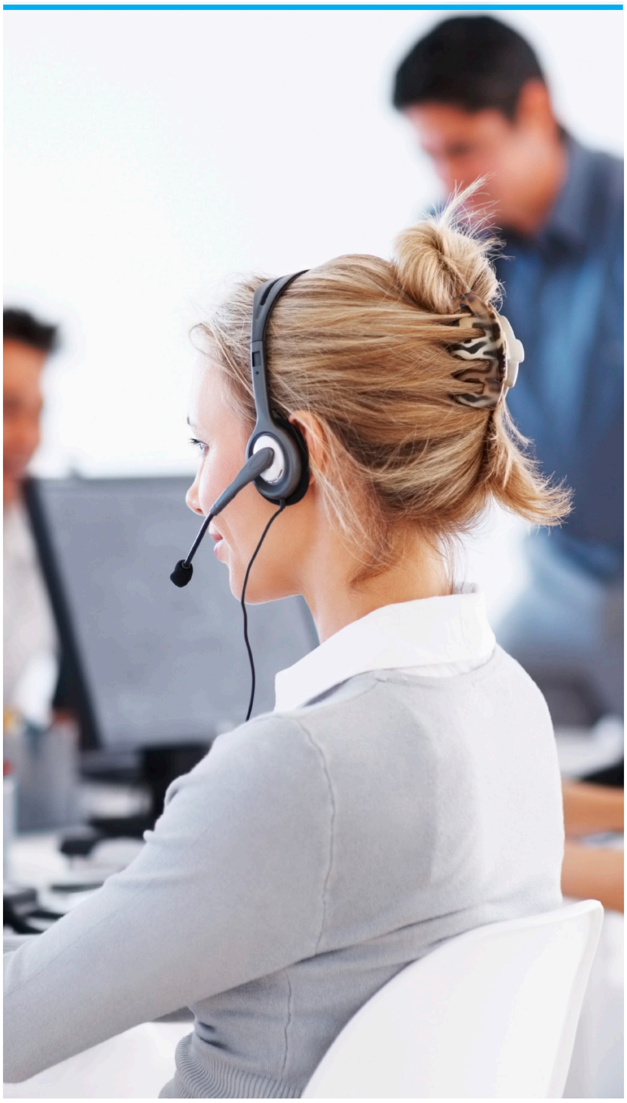
- Automation of 200 work places due to implementation of NAUMEN Contact Center platform
- Operational processing of more than 600 simultaneous calls
- The average waiting time does not exceed 15 seconds
- The share of missed calls does not exceed 5%
- The share of calls processed in the self-service systems increased by 15%, which allowed reducing the workload of operators, increasing the availability of call center
- Client support provided in the language selected in the Interactive Voice Response (IVR) menu: English, Romanian, Russian
- Operation of up to 1400 joint lines
- Continuous operation of the call center
- Single operator's workstation
- Assurance of communication via the following channels: email, SMS, chat

EFFECT OF IMPLEMENTATION

- Staff of each unit of Moldtelecom call center received an easy access to all the necessary business applications
- The share of manual labor decreased
- Improved efficiency in work with debtors due to predictive dealing and sending of notifications that include information about maturity of the existing debt
- Proportion of requests solved during the first time application to technical support (First Contact Resolution) had raised by 10% and the share of calls transferred to the second line of support had diminished twofold
- The system allowed automation of registration of requests of the help desk
- The average time of request processing had decreased by 20 seconds
- The share of high grades has considerably increased

FUNCTIONALITY OF THE PLATFORM

- Intelligent Call Routing
- Control of outbound call-down (manual, progressive, predictive)
- Interactive Voice Response (IVR) menu
- Recording and storage of conversations
- Graphic construction of conversation scenarios
- Unified data base for operators
- Web access to the reports on all the projects, including OLAP reports with the possibility of audition of conversations
- Quality assurance
- New call center platform is integrated with the main information systems of Moldtelecom: Billing (BillMaster, MindBill), IN-platform, BroadBandSupportManager, UniteInfo, ABR



ATM TECHNICAL SUPPORT & MAINTENANCE SERVICES

DAAC SYSTEM INTEGRATOR

DAAC System Integrator offers ATM Technical Support & Maintenance services increase uptime of ATMs and to maintain ATMs in a good state for a long period.

BENEFICIARIES OF THE SERVICE

- Moldova Agroindbank
- Victoriabank
- MobiasBanca GSG
- FinComBank
- Banca Comerciala Romana Chisinau
- ProCreditBank
- ComertBank

ADVANTAGES OF THE SERVICE

- High level of technical support offered by qualified specialists
- Assuring in-time delivery of original spare parts for ATMsand aftermarket support
- Software support and maintenance provided by certified specialists
- Highly standardized Call center & Help deskSupport and maintenance divided by levels (L1 - Help desk and FLM, L2 - SLM, L3 - Spare parts replacement, Supplier’s support)
- Mobile teams of qualified technical specialists, which serve the whole ATM network in the Republic of Moldova and nearby regions of Romania and Ukraine
- Unique service provider of the world-known ATM brands Diebold Nixdorf (Wincor Nixdorf) and NCR

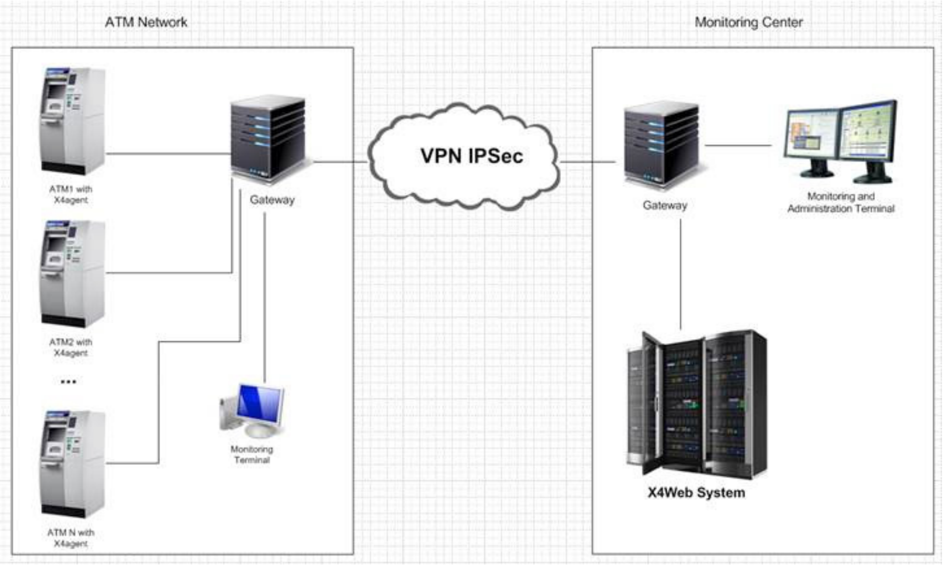
ATM TECHNICAL MONITORING BASED ON X4 MONITORING SOFTWARE

ATM Technical Monitoring based on X4 Monitoring Software represents high-quality solution for surveillance of ATM network.

BENEFICIARIES OF THE SERVICE

- Moldova Agroindbank
- ProCreditBank
- MobiasBanca GSG

SOLUTION ARCHITECTURE



ADVANTAGES OF THE SERVICE

- Obtaining the required level of ATM's uptime
- Minimization of technical intervention time (due to detailed problem report)
- Automatization of problems' registration (minimization of time spent by Bank's employees on technical issues)
- Reduction of time required to detect a problem from 1 hour (before X4 Monitoring system installation) to 5 minutes
- Detailed report of ATM operations (description of normal operations and problematic issues)

PERIOD OF REALIZATION

- Understanding Bank's requirements for the Technical Monitoring Solution – 10 days
- Collecting information regarding technical parameters of ATMs and Bank's network – 2 weeks
- Server-side installation – 2 days
- Client-side installation on each ATM – 6 hours per ATM
- Connection of the server and client sides, testing – 2 days
- Launch of the system in real-time operating mode – 1 day

Total implementation time – 45 Days

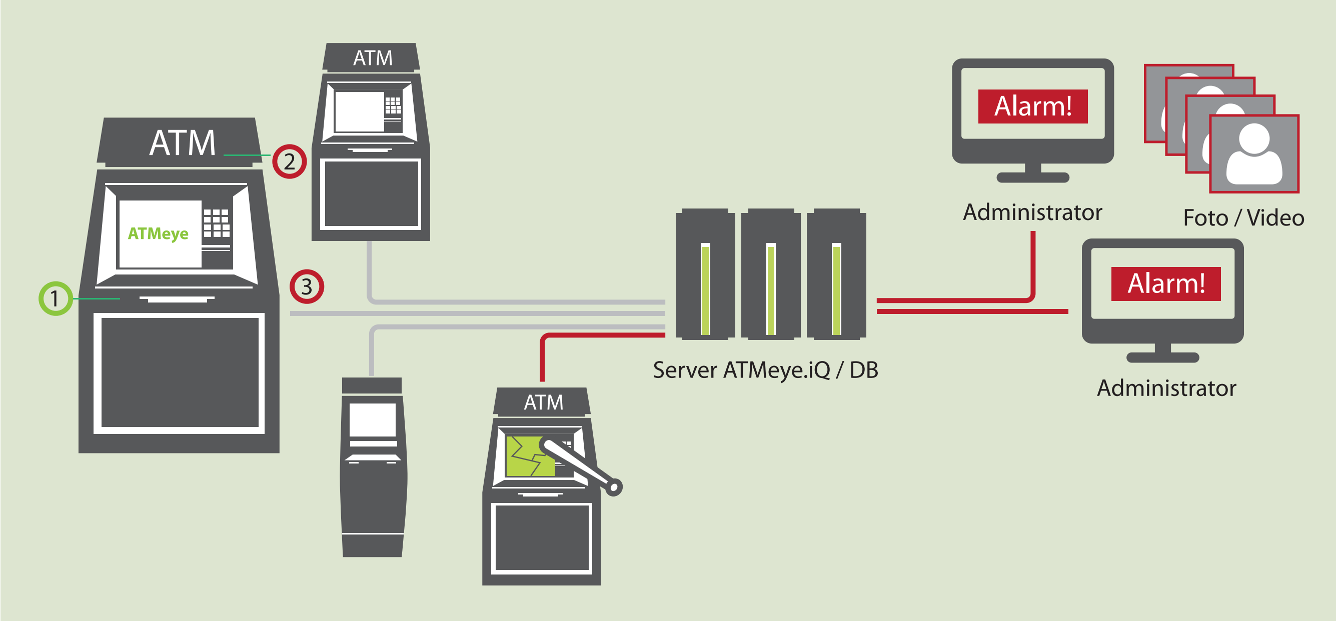
ATM SECURITY SYSTEM BASED ON ATMEYE.IQ SOLUTION

DAAC System Integrator provides ATM security services based on ATMEYE.IQ solution with the aim to increase the level of reliability of ATMs.

BENEFICIARIES OF THE SERVICE

- Banca Comerciala Romana Chisinau
- Moldova Agroindbank
- Victoriabank

SOLUTION ARCHITECTURE



ADVANTAGES OF THE SERVICE

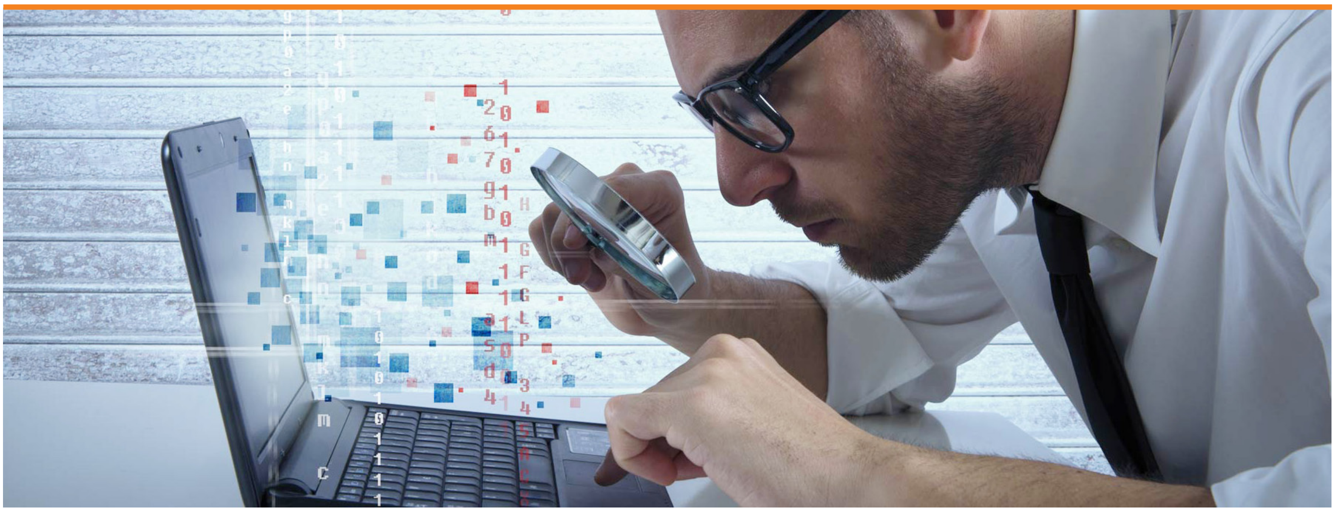
- Retention or return of blacklisted cards with immediate notification of the operator
- Convenient search of transactions in archived and non-archived data by card number, event, date, etc.
- Administration of users' rights
- Multivendor service (hardware independent)
- Full integration with self-service device software
- Generation of different kinds of reports
- Card numbers masking

PERIOD OF REALIZATION

- Understanding Bank's requirements for ATM Security Solution – 10 days
- Collecting information regarding technical parameters of ATMs and Bank's network – 2 weeks
- Server-side installation – 2 days
- Installation of client software and cameras – 1 day per ATM
- Connection between the server and client sides, testing – 2 days
- Launch of the system in real-time operating mode – 1 day

Total implementation time – 60 Days

NETWORK SECURITY LEVEL EVALUATION: PENETRATION TESTING



Penetration testing is one of the most popular services in the information security area. It implies the authorized attempt to breach the existing complex of information security infrastructure from an exterior or interior network, exploring vulnerabilities in the software of servers, network equipment and network protection tools. The general objective of penetration testing is to evaluate the security level of active network nodes in order to reveal vulnerabilities before real attackers can detect them. To do so, usually technical means of corporate network defense are tested; however, depending on the requirements, other network security aspects such as the level of employees' awareness of information security should also be evaluated.

Penetration testing can be conducted either as a component of ISO/IEC 27001 information security audit compliance, or as an independent test requested for justification of the network security improvement. In any case, it shall be executed for an independent evaluation of the security level of the information system.

Both automated tools and manual analysis methods are applied for penetration testing. The final report (result) of Penetration testing consists of the following parts:

- the applied testing methodology
- the management report, which contains conclusions about the general level of information security
- the technical report, comprising detailed description of detected vulnerabilities
- description of testing process, presenting information about all the vulnerabilities detected and the results of their exploitation
- recommendations concerning elimination of detected vulnerabilities

Assessment of the network infrastructure protection level, which is obtained as a result of a Penetration test, gives the Client the possibility to elaborate an Information Security Strategy based on in-depth analysis of possible consequences of exploitation of vulnerabilities detected by attackers; also, to optimize expenditures related to information security by redirecting finance for the most critical domains, which require immediate protection.

PENETRATION TESTING TOOLS

Automated security scanners are used for optimization of testing process. These scanners contain a relevant database of vulnerabilities, which is permanently updated by developers. The scanners detect hosts on which server services are running and checks them for presence of such vulnerabilities as cross-site scripting, directories view and detection, SQL command entry, etc. The software is also performing testing of HTTP authentication for detection of unsecure settings and weak passwords and reports presence of obsolete security software on server, which needs to be updated or corrected.

KEY FEATURES OF PENETRATION TESTING TOOLS:

• **Complete services identification on random ports**

Gives the possibility to check for presence of vulnerabilities of services with complex configuration, i.e. when services have randomly chosen ports

• **Heuristic method of services name and type identification** (HTTP, FTP, SMTP, POP3, DNS, SSH), which does not depend on services standard query responses

This method is used for detection of a real server name and for consistent checking process in case when configuration of WWW-server hides or changes a real name of a server

• **RPC services processing and their complete identification**

Allows recognition of RPC services, search of vulnerabilities of those services and specification of detailed configuration of PC

• **Check of password weakness**

Performs optimized selection of passwords in all services requiring authentication, which allows detecting weak passwords

• **In-depth analysis of web site content**

Analysis of all HTTP server scripts (primarily users') and search of various vulnerabilities: SQL injection, code injection, random software run, receiving of files, cross-site scripting (XSS), HTTP Response Splitting

• **Analyzer of HTTP servers structure**

Allows search and analysis of directories available for viewing and recording, which enables finding weak spots of configuration

• **Non-standard DOS-attack tests**

There is an option to include checks for "service denial", which account for methods of previous attacks and hackers' techniques

• **Special mechanisms that allow to reduce false positive rate**

Different types of tests employ methods that were specifically elaborated for those tests in order to reduce the likelihood of false positives

• **Daily update of security database (adding new vulnerabilities and new checks)**

Authentic technology of software update allows users to have access to daily updated database of vulnerabilities without the need to stop the software and requiring minimal traffic and time inputs; moreover, it allows users to have regularly updated software modules

TESTING PROCEDURE

Technological testing for evaluation of vulnerabilities of an external or internal network infrastructure could be performed either with notification of Client's technical specialists and users of the system or without notification.

Testing procedure can be implemented in four phases according to the following plan:

PHASE 1. PRELIMINARY PREPARATION

Obtaining preliminary information about Client's network:
- network infrastructure research (network diagram development)
- servers infrastructure research (determination of types of devices, Operation Systems and applications)
- preparation for testing (elaboration of a check list)
- ensuring access to the application

PHASE 2. TESTING REALIZATION

- implementation of vulnerability testing (ports scanning, services identification, detection of vulnerabilities)
- analysis of preliminary results of tests (analysis of detected vulnerabilities, configuration and software vulnerabilities)
- repeated testing

PHASE 3. PREPARING REPORTS

- management report
- technical report

PHASE 4. PREPARING RECOMMENDATIONS

- elaboration of general recommendations for management team regarding improvement of security of infrastructure
- elaboration of recommendations for technical staff regarding minimization of impact of detected vulnerabilities

Critical vulnerabilities detected by instrumental analysis of security scanners and additional tools that automate several scenarios of exploitation and detection of vulnerabilities, at Client's request, could be checked for possibility of obtaining control over data, system penetration or violation of normal operation mode of an application.

The goal of the above mentioned test is to check possible errors of security scanners analysis, i.e. type I errors or False Positive errors, when detected vulnerabilities don't pose risks and effort and financial resources dedicated to their elimination are redundant.

PHASE 5 (OPTIONAL). EXPLOITATION OF VULNERABILITIES

- attempt to penetrate system, attempt to get control over data
- demonstration of possible penetrations
- analysis of final results

TESTING RESULTS

The final analytical conclusion for management team and technical experts represents the result of a Penetration test.

The report for Management Team consists of:
- overall testing results
- overall security level evaluation
- general recommendations dedicated to security infrastructure perfection
- conclusions

The report for Technical Experts consists of:
- specification of testing techniques
- testing features
- detailed testing results distributed by active nodes
- security level evaluation for each of testing nodes
- recommendations regarding elimination of detected vulnerabilities or minimization of possible negative effect related to their exploitation