The 7th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 15th 2012

CONSIDERATION ON ANTIVIRUS PROTECTION AT ARMAMENTS DEPARTMENT

Lt.col.eng. Lucian Bibo

Ministry of National Defence / Armaments Department/Bucharest

Abstract:
Network's infection by viruses is a cause of majority companies and governmental organizations losses. In some circumstances such infections appear despite antivirus protection existing on workstations. Ones can ask: *Okay, but I have antivirus on each station, though I was infected. Why?* The answer is many times simple: because the solutions were not correctly configured, installed and/or were not thought to work together. In this paper will be provided some piece of information about how these issues are approached at Armaments Department.

Key words: antivirus, network, protection, security, Armaments Department, BitDefender

1. Introduction

Now more than ever, institutions are concerned about the security. The number, variety and strength of the threats to computer and network security have dramatically increased and businesses need to be prepared against an ever-changing landscape of attacks.

Armaments Department is the structure of Romanian Ministry of National Defence[MoND] responsible for the management of major defence acquisition programs, R&D, testing and evaluation of military equipment and technologies, contracts for domestic and foreign acquisitions, quality assurance and surveillance at domestic suppliers. It also coordinates Military Technical Academy, Military Equipment and Technology Research Agency and C.N. Romtehnica S.A.

Led by a secretary of state, Armaments Department consists of three main directorates (planning, R&D and contracting) and independent subordinate microstructures (including IT service).

IT infrastructure implemented to sustain organization's activities includes the following systems, organized according operational needs:

- LAN to access public INTERNET services,
- LAN interconnected with INTRAMAN, the private MoND restricted WAN,
- independent workstations (desktops and mobiles).

Having in mind the value of information stored and processed, a real growing asset despite the other lacks, the antivirus protection is very important. Safety is not a privilege is a must.

CONSIDERATION ON ANTIVIRUS PROTECTION AT ARMAMENT'S DEPARTMENT

Security doesn't have to be complicated, time consuming, or expensive. Government knows that there is a real need for security, but may be skimpy about cost issues.

2. Antivirus protection

With computer literacy increasing dramatically and the line between private and business use of computers and networks blurring, organizations need to keep a close eye on their employee's activities on their IT infrastructure and ensure that their security is not at stake.

There are many solutions, but all have a single starting point, namely that of a thorough analysis of network status, of software requirements and practical arrangements for security. Following this analysis supply may develop based on which you can go and search companies' offers to provide corporate antivirus solutions that meet the requirements set.

Now comes the most complicated part in the bid selection. At this point you should take into consideration not only the price you can get for a certain number of licenses, very important is what you get for that price!

Technical support, upgradeable and responsiveness of the company providing at the time of infection is particularly essential.

Since 2002, following a public acquisitions procedure, a virus protection solution from the Romanian software solution provider Softwin, a.k.a. BitDefender, has been implemented at Armaments Department.

At the beginning, the protection was configured for each workstation and server individually. As systems developed, both hardware and software, in conditions of increasing threats, we fully benefited of provider's launch of more complex products with integrated management features.

I will not make an in-depth description of products but leave the discovery temptation to those interested. What I intend to do is to introduce some general information about the software solution and reveal some particular aspects witch finally allowed a real cost effective antivirus protection implementation.

2.1. Antivirus Architecture for networks

The core element for networks protection is BitDefender Client Security, a robust and easy-to-use business security and management solution, which delivers superior proactive protection from viruses, spyware, rootkits, spam, phishing and other malware.

It enhances business productivity and reduces management and malware-related costs by enabling the centralized administration, protection and control of workstations inside companies' networks.

BitDefender Client Security includes the following components:

- Management Server
- Client products
- Management Agent
- Management Console
- Deployment Tool
- Update Server

2.1.1. Management Server

Management Server is the main component of BitDefender Client Security. Its purpose is to manage all security solutions inside a network based on customizable security policies. Using Management Server, client products can be remotely installed and managed.

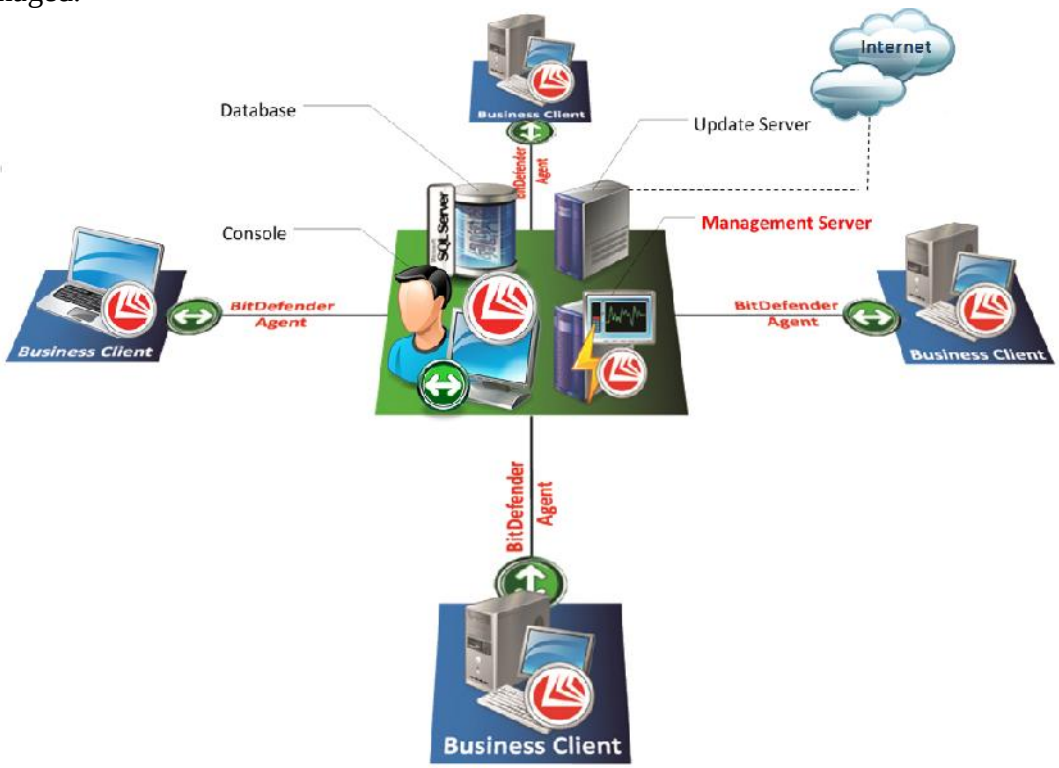

Figure no.1: Remotely Install and Manage BitDefender Client Products

The "brain" of the product

The policies received from the user through the management console are forwarded to the workstations in order to be executed, while the information received from the workstations is processed by Management Server. The information is then forwarded to the management console where it can be viewed and interpreted by the administrator.

Management Server can be dynamically extended to perform various other security-related policies that users may need. Clients can also be managed from a workstation other than Management Server.

Connected to Database

Management Server will stay permanently connected to a database (for example MS SQL Server Database) that stores information about all product configuration files. In this way, BitDefender Management Server can manage a huge amount of information in the shortest possible time.

Password-protected

Management Server is password-protected in order to prevent unauthorised access.

2.1.2. Client Products

A client product is a product that Management Server manages remotely, through policies.

BitDefender Client Security smoothly integrates with and manages:

- Workstation Client Products :
  - BitDefender Business Client
- Server Client Products (Gateway Level) :
  - BitDefender Security for Mail Servers (Windows, UNIX)
  - BitDefender Security for Exchange
- Server Client Products (File Server Level)
  - BitDefender Security for File Servers (Windows)
  - BitDefender Security for Samba
  - BitDefender Security for SharePoint

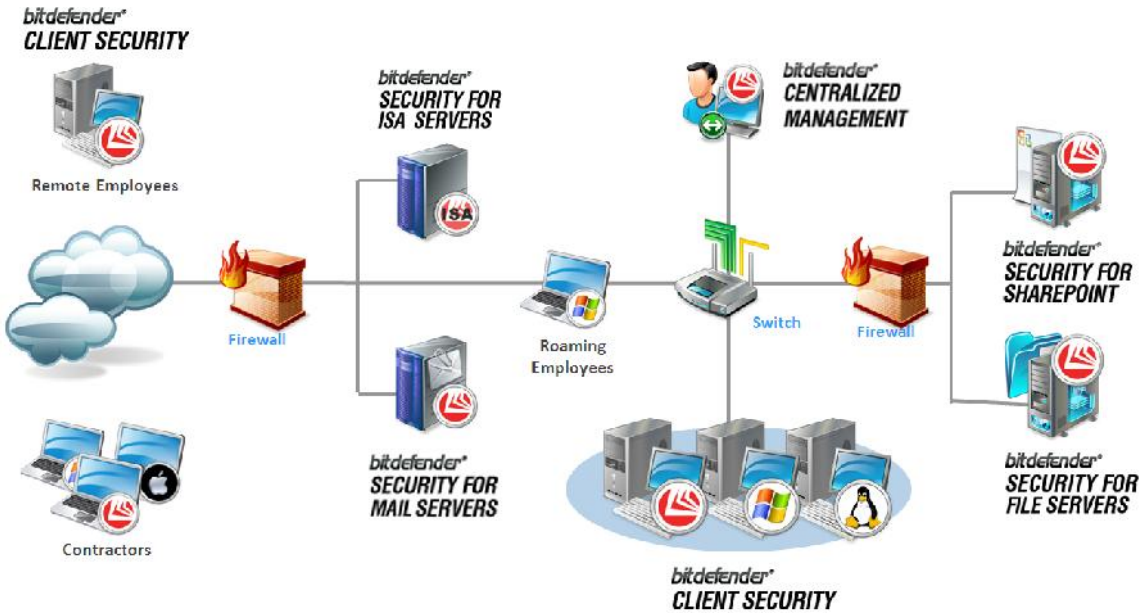

Figure no.2: BitDefender Client Products

2.1.3. Management Agent

Management Agent is the component deployed on each workstation to be managed by Management Server. It is used to ensure communication between Management Server and the client products installed on a specific workstation. It fulfils three main functions:

- queries Management Server to learn the security policies that need to be applied to the local workstation,
- applies the security policies received from Management Server,
- sends the results of the applied policies to Management Server .

2.1.4. Management Console

Management Console represents the graphical user interface (GUI), created to allow the administrator to interact with BitDefender Management Server.

By using the management console you can:

- visualize the entire network (managed computers, computers that are not currently managed by Management Server, computers excluded from management),
- remotely deploy Management Agent on detected network computers or on computers from Active Directory,
- remotely deploy BitDefender client products on managed computers,
- set Management Server to automatically deploy Management Agent and Business Client on newly detected computers,
- find out detailed information about a managed computer,
- assign policies to managed computers or to computers from Active Directory in order to configure and even to install client products,
- run management tasks on managed computers in order to remotely perform administrative tasks,
- check the results of the assigned policies and network management tasks,
- configure Management Server and monitor its activity,
- obtain centralized easy-to-read reports regarding the managed computers,
- remotely remove client products installed on managed computers.

2.1.5. Deployment Tool

Deployment Tool is an independent component that helps to automatically install, remove or repair products on remote network computers. This tool also enables to create unattended installation packages for use on offline computers (or when remote installation fails).

2.1.6. Update Server

Update Server is an independent component that allows you to set up a BitDefender update location within the local network. In this way, you can reduce Internet traffic because only one computer will connect to the Internet to download updates while the others will update from this local mirror. Moreover, updates will be performed faster and even on the computers that are not connected to the Internet.

2.1.7. Supported Client Products

Management Server smoothly integrates with and manages both workstation and server security solutions.

Business Client

BitDefender Business Client integrates antivirus, firewall, antispam and antispyware modules into one comprehensive workstation security package, tailored to meet the needs of corporate computer users.

Server Client Products

Security for Mail Servers

BitDefender Security for Mail Servers protects Windows or UNIX-based mail servers for known and unknown security threats with award winning proactive antivirus, antispyware, antispam, antiphishing, content and attachment filtering technologies.

The solution secures organization's email services and provides increased productivity by blocking spam and providing common centralized management tools.

Security for Exchange

BitDefender Security for Exchange safeguard's your organizations critical messaging services to protect against email-borne viruses, spyware and spam. Integrating seamlessly with Microsoft® Exchange Server, BitDefender Security for Exchange combines malware protection, antispam, antiphishing, and content filtering technologies to increase productivity and ensure the overall integrity of your email platforms.

Security for File Servers (Windows)

BitDefender Security for File Servers provides optimized protection of both the server operating system and data file structure for critical back-end systems. Easy to install, configure and maintain via the centralized management console, BitDefender for File Servers protects against viruses, spyware and rootkits to minimize the impact of malware propagation throughout the network.

Security for Samba

BitDefender Security for Samba enables organizations to deploy antivirus and antispyware protection for their Samba network shares running on Linux, FreeBSD and Solaris systems. Deployed and maintained centrally within the network, Security for Samba scans cross-platform data structures and file stores for malware, keeping network users safe from virus infection.

Security for SharePoint

BitDefender Security for SharePoint provides proactive protection of SQL document repositories against known and unknown viruses, spyware, Trojans and root kits.

Real-time, optimized session-based scanning of uploaded, downloaded or accessed files helps to prevent Microsoft SharePoint deployments from storing and sharing of infected files within the network.

2.2. Antivirus for Stand Alone Computers

Options for protecting independent computers were for standalone category products.

BitDefender released three type of products, mostly targeted for home users. Taking into consideration the operational requirements (working without any communication), the option was for the less complex : Bitdefender Antivirus Plus.

Some of the product characteristics are the following:

- Active Virus Control - A proactive, dynamic detection technology which monitors processes' behavior in real-time, as they are running, and tags suspicious activities.
- USB Immunizer - Immunizes any Flash Drive from viruses, when connected to computer,
- Rescue Mode - If e-threats, such as rootkits, cannot be removed from within the Windows operating system, the computer is re-booted in rescue mode—a trusted environment which is then used for cleanup and restoration,
- Vulnerability Scanner - Checks for missing or outdated security software, missing Windows security patches, as well as potentially unsafe system settings.

A second option, in the future, could be Bitdefender Total Security that integrates extra features which would be of inters:

- File Shredder – Completely erase sensitive stored files on PC or media,
- File Encryption – Locks up confidential files in an encrypted vault.

2.3. Implementing on LAN to access public INTERNET

LAN to access public INTERNET services consists of one Microsoft ISA server, two domain controllers, one file server, one web server hosting Armaments Department internet website www.dpa.ro, one server for webmail (HMail with SquirellMail) and client workstations.

The implementation is presented in Table 1.

Equipment	**BitDefender product**							
	Management server	**Management agent**	**Update server**	**Managent console**	**Security for ISA**	**Security for File Servers**	**Security for Mail Servers**	**Business Client**
ISA server					X	X		
1st domain controller		X				X		
2nd domain controller	X	X	X	X				
Web site server		X				X		
WebMail server		X				X	X	
Workstations				X*				X

** installed only on administrators workstations*

Table 1

Using management server, computers were organized in specific groups according to the structure the organization and the rights to access mobile storage devices.

Clients can be sorted by name, description, IP address, the time when the agent last synchronized, agent version etc.

A set of default policies were created and tasks are assigned to specific clients or to entire client groups (even to the entire Managed Computers group).

BitDefender Business Client can operate in two modes: restricted user and power user. In the restricted user mode, the user cannot configure the product, but only perform basic tasks, such as launching a default scan task, updating BitDefender or backing up data. In the power user mode, the user has full control over BitDefender Business.

Except administrators' workstations, all business clients operate in the restricted user mode.

Real time protection is set on every client and can be changed only by power users.

First action, when a file is detected as infected is set to *disinfect* and second to *delete*, this last option being preferred instead of quarantine.

All alerts are sent by e-mail to administrators group.

Using tasks, deep scans are assigned and executed on servers every night and once a week on workstations.

The first update location is set to the internal update server and secondary the internet site of the provider (https://upgrade.bitdefender.com). Clients are set to search for update every hour.

2.4. Implementing on LAN interconnected with INTRAMAN

LAN interconnected with INTRAMAN consists of one domain controller, one Microsoft Exchange server, one Windows Share Point & file server, one application server, one WSUS server and client workstations.

Table 2 summarizes LAN –INTRAMAN implementation.

Equipment	BitDefender product							
	Management server	Management agent	Update server	Manageent console	Security for SharePoint	Security for File Servers	Security for Exchange	Business Client
Domain controller								
Exchange server		X				X	X	
WSS & file server		X			X	X		
Applications server		X				X		
WSUS	X	X	X	X		X		
Workstations				X*				X

** installed only on administrators workstations*

Table 2

The domain controller is managed exclusively by INTRAMAN administrators who are responsible with all security of this server. Only issue of concern is the compatibility of antivirus protections.

Using management server, computers were organized in specific groups according to the structure the organization.

Access to mobile storage devices is allowed only at the transfer station. Except administrators, all business clients operate in the restricted user mode.

Some shared folders from application server are locally mapped as network drives on few workstations. In order to avoid simultaneously double scanning (by file server and client antivirus) a set of exclusions were established and assigned using WMI policies.

A set of exclusion is also implemented in order to make possible the normal function of WSS and Exchange servers.

Real time protection is set on every client and can be changed only by power users. Considering the LAN and potential threats, the following modules where inactivated: antispam filters, antifishing both on Security for Exchange and Business Clients.

The first action when a file is detected as infected was set to *disinfect* and second to *delete*.

All alerts are sent by e-mail to administrators group.

Using tasks, deep scan are performed on servers every night and once a week on workstations. The internal update server is the single update location. Updates are manually transferred from online Internet update server to the intranet update server, using mobile storage, at least once a week. Clients are set to search for update every day.

2.5. Implementing on independent workstations

Bitdefender Antivirus Plus is used for protecting stand alone computers.

Real time protection is set on every client and can be changed only by power users. Considering potential threats, some modules where inactivated: antispam filters, antifishing, firewall, parental control. Mobile storage are automatically scanned each time are used in system.

Automatic update is turn off. Updates are manually transferred from internet site of the provider (https://upgrade.bitdefender.com), using mobile storage, and installed at least once a week.

First action when a file is detected as infected was set to *disinfect* and second to *delete*.

Using tasks, deep scans are automatically performed twice a month.

3. Organizational measures

Some organizational measures complement software installation in order to provide a more safety environment.

Procedures for installing, for reporting and intervention were issued; administrators and user has been instructed how to react in specific conditions (eg. when viruses are detected or different tasks are lunched etc.).

At least once a day administrators verify management server reports, logs etc.

Duties to update products and viruses signatures on systems without internet connections and keep the track were establish.

4. Partnership

As previously mentioned, technical support, upgradeable and responsiveness of the company is particularly essential. By contract, two type of support are provided: online assistance and onsite intervention.

Online assistance is provided via e-mail or chat, a tracking system providing traceability from the notification to the resolution.

Onsite intervention is performed each time online assistance is not enough or specific needs require it.

Being both local provider and producer brings lots of advantages and reduces time to communicate and solve problems.

In an unwanted situation of infection, specific targeted disinfection tools are made available in time. For example, that was of a great help when systems where infected with Confiker. Normally it shouldn't happen, but because of budgetary restrictions, expired licenses where not renewed for more than 2 months and systems get infected. Using the tools provided, despite the contractual situation, all systems (more than 250 workstation in both networks) where disinfected in less than a three days.

Access to the latest versions of products is implicit within the contractual framework and a special discount is available for new products. Access to beta releases is also provided. That facilitated the possibility to test and familiarise with antivirus solution for virtualized environments.

An widening direction for future collaboration would be products customisation in order to make possible the use of MoND's own algorithms in File Shredder and File Encryption features.

5. Conclusion

Organization's growing dependence on IT and IT-based controls, information and IT security risks increasingly contribute to operational and reputational risk.

Even security is an internal issue (it can't be bought), a cost effective antivirus protection is of crucial importance and relies on technical measures, procedures, personnel training and responsiveness of the provider.

Leaders at Armaments Department understood the legal, managerial and operational considerations that converge in an enterprise security program and provided sufficient resources to implement and maintain an adequate antivirus protection.

References:

[1] BitDefender site , http://www.bitdefender.ro