Dr.WEB®
since 1992

Defend what you create

DWCERT-070-3
Enterprise anti-virus protection solutions

Qualification: Certified enterprise anti-virus security engineer

Contents

I. Modern virus threats. Informational resources about viruses . . . 3
II. Points of intrusion in a corporate network . . . 9
III. Company tasks. Actual tasks in relation to the structure of a corporate network . . . 12
IV. The structure of a local network . . . 15
V. Russian legislative requirements for the field of anti-virus security . . . 18
VI. Errors made when implementing an anti-virus system for a local network . . . 21
VII. General requirements when implementing an anti-virus protection system for a local network . . . 25
VIII. A description of network hosts and principles of protecting them . . . 28
Workstations and mobile devices . . . 28
Servers . . . 32
Mail servers . . . 36
Mail gateways . . . 40
Internet gateways . . . 42
IX. Doctor Web virus-related computer incident (VCI) expert consultations . . . 44
Cyber fraud and virus-related computer incidents . . . 44
IT security response service . . . 45
VCI investigations . . . 45
X. Rules of conduct after a VCI . . . 48
Money stolen from online banking systems . . . 48
Encoder Trojan encrypted files . . . 49
Blocker Trojan blocked access to Windows . . . 50

06.02.2018

I. Modern virus threats

MYTH

Viruses are written by individual hackers.

The time when programmers acted alone is long gone. Today's malware is being developed not just by professional virus writers; this is a well-organised criminal industry involving highly qualified system and application developers.

Structural elements of some criminal organisations

In some cases, the roles of attackers inside criminal organisations are as follows:

1. **Organisers** – people who organise and control the process of creating and using malware. Their malicious software can either be used directly or sold to other criminals or their organisations.

2. **Participants:**
   - Malware developers
   - Malware testers
   - Testers of vulnerabilities in operating systems and application software for criminal purposes
   - «Experts» on the use of virus packers and encryption
   - Malware distributors and social engineering experts
   - System administrators who control botnets and ensure a secure distributed operation within acriminal organisation.

Such labour organisations let criminals test their malware against all current anti-virus solutions. Hackers test malicious software against current anti-virus versions to ensure their malware can avoid detection. No matter how well an anti-virus performs in tests, it will be unable to neutralise this type of threat.

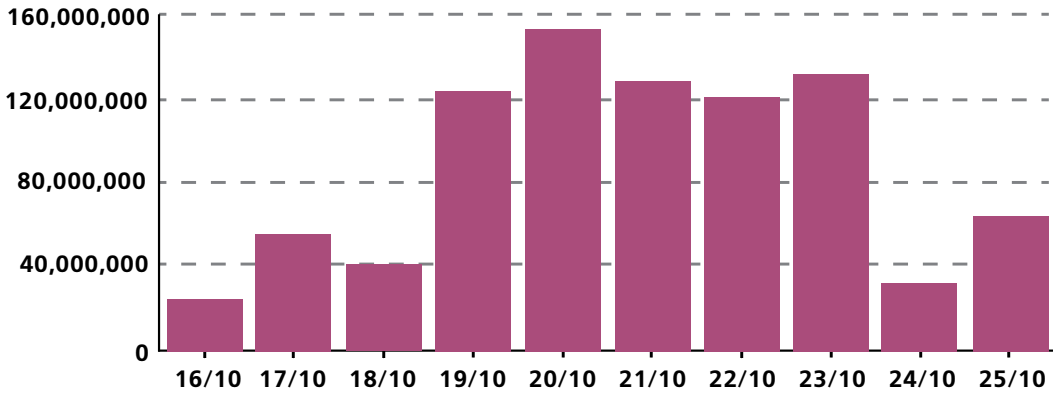
In addition, criminals now tend to create targeted threats—malicious programs designed to infect specific groups of users (e.g., bank customers). Typically, these are sophisticated malicious programs that don't disrupt the operation of the machines they infect and at the time of infection are not identifiable by anti-viruses, allowing them to remain undetected for a long period of time.

As a result of this industrial-scale workflow to develop and release malware, only programs that can't be detected by anti-viruses (before the corresponding updates are delivered)—even using heuristic analysis—are released into the wild. Thus, the number of malicious programs that **can't currently be detected has increased dramatically.**

With malware development having evolved into a criminal business, anti-virus comparative tests can no longer serve as the criteria for selecting an anti-virus software product.

Thanks to the fact that criminal groups involved in the development and spread of malware are so efficiently organised, malware can be churned out quickly. This has led to explosive growth in the number of malicious programs created by hackers and a subsequent increase in the number of signature records being added daily to the virus database.

06.02.2018



Due to Dr.Web Virus Analytics web-site

Facts

- The Doctor Web virus-monitoring service collects samples of malicious programs all over the Internet.
- Every day Doctor Web's anti-virus laboratory receives on average over 100,000 malware samples.

For more information visit: http://live.drweb.com .

Virus analysts are not magicians; they can't instantly process the thousands upon thousands of suspicious files received daily. Automated solutions processing the incoming stream of suspicious files provided by anti-virus companies are essential elements of anti-malware protection. The quality of these systems is of no less importance than the quality of the commercial products running on user computers.

MYTH

An anti-virus should detect every single virus.

The prehistory of this myth

In the anti-virus industry, supposedly independent testers have been conducting so-called comparative tests on the ability of anti-viruses to detect viruses. Such tests involve collections of viruses and malicious programs; anti-viruses are updated to their current state and scan collections. To win a comparative test, an anti-virus must detect 100% of the viruses from the collections.

Test specifics are as follows:

- none of the testers can guarantee that its own collection contains purely malware;
- these tests allow only one of an anti-virus's features to be demonstrated—i.e., threat detection;
- such tests allow the performance evaluation of only one component, among the multiple components incorporated into an anti-virus—the file monitor or the scanner; in other words, an anti-virus is tested for its ability to combat threats known to be inactive.
- such tests do not demonstrate how an anti-virus behaves under real computer virus-infection conditions and how it can cure a particular virus or detect unknown threats.

Such tests have created this dangerous misconception.

Facts

- Technologically sophisticated and highly dangerous viruses, including rootkits, are created for commercial purposes. Virus writers scan them with all known anti-viruses before releasing them into the wild. After all, they need a virus to carry out its work on an infected machine for as long as possible. From the point of view of virus makers, an easy-to-spot virus is a bad virus. That's why many malware samples are not detected by anti-viruses before they get into an anti-virus lab.
- A virus can penetrate a computer via a zero-day vulnerability that is currently known only to the virus writer or for which the software developer has not yet released patches, or using social engineering techniques—i.e., it will be launched by a user who has the ability to disable the anti-virus's self-protection mechanism.

MYTH

Anti-viruses use virus signatures (i.e., records in virus databases) to catch viruses.

If this were so, an anti-virus would be helpless in the face of **unknown** threats.

However, an anti-virus is still the best and the only effective means of protecting against all types of malicious threats—and most important—against both those that are **well known** and those that are **unknown** to the virus database.

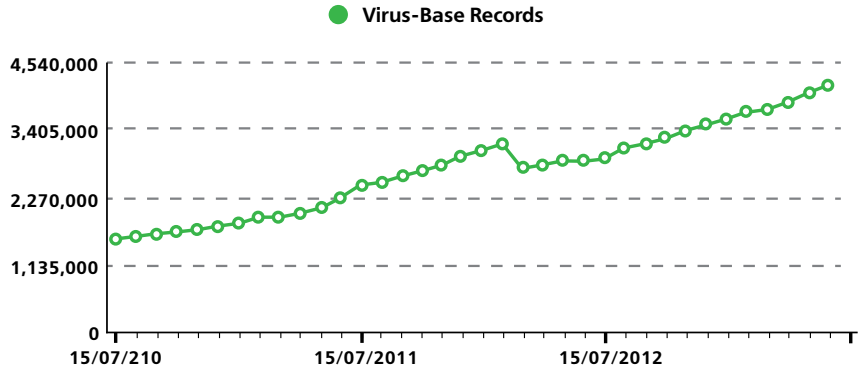
A myriad of effective, **non-signature technologies** is used to detect and remove unknown **malware.** Together, these technologies make it possible to detect the newest (unknown) threats that have yet to be registered in the virus database. We'll describe just a few of these technologies.

- **FLY-CODE technology** ensures the high-quality scanning of packed executables; this technology unpacks any (even non-standard) packers by using virtualisation for file execution—this makes it possible to detect viruses that are packed even by packers unknown to Dr.Web anti-virus software.
- **Origins Tracing** treats a scanned executable as a specific sample which it then compares against the database of known malicious programs. This technology makes it highly likely that viruses not yet added to the Dr.Web virus database will be detected.
- **Structural entropy analysis** detects unknown threats by arranging pieces of code in objects protected with encryption compression.
- **ScriptHeuristic** prevents any malicious browser scripts and PDF documents from being executed, without disabling the functionality of legitimate scripts. It protects against infection by unknown viruses that try to access systems via web browsers. It works independently of the Dr.Web virus databases, in any web browser.
- **Our traditional heuristic analyser** features routines used to detect unknown malware. The heuristic analyser relies upon knowledge (heuristics) about certain properties typical of virus code and, vice versa, properties that are extremely rare in viruses. Each of these attributes is characterised by its «weight» – that is to say, by a number whose module refers to the importance and severity of the attribute; and its sign, respectively, indicates whether that attribute confirms or refutes the hypothesis on the possible existence of an unknown virus in the code being analysed.

- **An execution emulator module** is used to detect polymorphic and highly encrypted viruses when the search against checksums cannot be applied directly or is very difficult to perform (because secure signatures cannot be built). This method involves simulating the execution of analysed code by an emulator—a programming model of the processor (and, in part, of the PC and OS).

Facts

- Dr.Web anti-viruses have a record-low number of virus definitions in their database; just a single entry allows tens, or hundreds, or even thousands of similar viruses to be detected. The fundamental difference between the Dr.Web virus databases and the virus databases of other anti-virus programs is that their (Dr.Web virus databases) smaller number of virus entries allows them to detect the same quantity (or even greater quantity) of viruses and malicious programs.
- Doctor Web is constantly developing malware-detection technologies and releases new versions of its anti-virus engine regularly. But the release of a new anti-virus engine version signifies more than just the delivery of new technologies; it means optimised code and fewer virus entries, which also positively impacts performance.



According to live.drweb.com

New detection technologies also slow the growth in the number of entries: Dr.Web uses fewer records to detect more malware!

- Even if no definition for a particular virus is present in its virus database, Dr.Web will most likely detect the virus using the multiple technologies implemented in its anti-virus engine.
- Dr.Web virus databases are devised in such a way that adding new entries doesn't reduce scanning speed!

What are the advantages of a small virus database with fewer entries (than our competitors have)?

- High-speed scanning
- Lower system requirements
- Saved disk space
- Lower updating traffic
- Future modifications of existing viruses will be detected

IMPORTANT!

Every day millions of people around the world use the unique product Dr.Web CureIt!, created specifically to cure infected computers running other anti-viruses.

MYTH

Viruses are long gone!

Indeed, over 90% of today's threats cannot be called viruses in the strict sense of the term since they do not have the ability to self-replicate (copy themselves without user intervention). The majority of today's threats are Trojan programs, which belong to a category of malicious programs and can cause serious damage to the owner of an infected computer.

Dangerous Trojans:

1. Are invisible both to the user and to some anti-viruses.
2. Are capable of stealing confidential information, including passwords used to access banking and payment systems, and cash from bank accounts.
3. an download other malware and even prevent an operating system from working properly.
4. Can be ordered by attackers to completely paralyse a computer.
5. When created, such programs usually cannot be detected by anti-virus engines. Moreover, some of them try to remove anti-viruses.

Facts

- Up to **70%** of infections in corporate LANs isolated from the Internet are caused by infected removable media—people spread Trojans from one PC to another **with their flash drives.**

IMPORTANT!

Indeed, an anti-virus can fail to detect the latest malicious program designed for covert intrusion, but no other software, except an anti-virus, can cure a system that has already been compromised by a Trojan.

MYTH

A virus's actions are usually visible on a computer. If my computer gets infected, I'll immediately know it and take appropriate action.

Facts

- Today's malware is often designed to maintain a long-term presence on a victim's computer. Therefore, it doesn't just operate invisibly and go undetected by many anti-viruses for some time after its creation; some malware programs can even fight with their competitors and remove other malware. There are even malicious programs that close vulnerabilities on the target computer!
- For example, Trojan.Carberp was designed to steal money. When it starts up on an infected machine, it undertakes several steps to avoid being detected by control and monitoring systems. After launching itself successfully, the Trojan injects itself into running applications and shuts down its primary process. Thus, the Trojan conceals its activity inside third-party processes.

The myth that any virus can easily be noticed has been dispelled once and for all.

MYTH

Even if a computer is infected, it's cheaper to recover Windows from the backup than it is to buy an anti-virus.

Threat

Even if a computer is infected, it's cheaper to recover Windows from the backup than it is to buy an anti-virus.

MYTH

Even if a computer is infected, it's cheaper to recover Windows from the backup than it is to buy an anti-virus.

Even if the data on a PC hasn't been backed up, it's not a problem. If your system was infected before you installed Dr.Web, Dr.Web will cure it, and your computer will operate normally again. To cure an active infection, it's enough to run a quick scan of your computer, and all the threats found will be neutralised. Even curing multiple computers in a network will take less time than restoring a system from a backup! And with Dr.Web, the following occurs:

- infected files are cured;
- the Windows registry is automatically corrected;
- malware services are automatically removed;
- rootkits and bootkits are automatically removed.

Informational resources about modern virus threats

- Doctor Web anti-virus laboratory: http://live.drweb.com
- Descriptions of viruses and other malware: http://vms.drweb.com/search
- Reviews about viruses and spam: http://news.drweb.com/list/?c=10
- Real-time threat news: http://news.drweb.com/list/?c=23
- Subscribe to Doctor Web virus news and reviews: https://news.drweb.com/news/subscribe
- Send a suspect file to the virus laboratory for analysis: https://vms.drweb.com/sendvirus

Online Dr.Web scanner: http://vms.drweb.com/online

06.02.2018

II. Points of intrusion in a corporate network

Relying on **outdated information** about how malware penetrates systems and what it is capable of is what causes most companies to make grave mistakes when it comes to establishing an anti-virus protection system.

To effectively protect a corporate environment, security specialists need to know **how malware penetrates** local networks. Today the main malicious access points are:

1. Vulnerabilities

A vulnerability is a software flaw that can be exploited to compromise the software's integrity and render it non-operational. Vulnerabilities exist in every piece of software. There are no invulnerable programs.

Modern virus writers exploit vulnerabilities not only in operating systems but also in applications (browsers, office products, such as Adobe Acrobat Reader, and plug-ins for browsers to display flash).

A virus can access your computer by exploiting a zero-day vulnerability (a vulnerability that is still only known to virus writers or hasn't yet been closed by the software vendor), or a user may fall for a social engineering trick and launch a virus file and even disable their anti-virus's self-defence.

IMPORTANT!

An anti-virus is the only software that can clean a system of the malicious software that has penetrated it by exploiting a vulnerability.

IMPORTANT!

No other software requires such frequent updating as an anti-virus.
New viruses are being written all the time, and virus databases are updated at a very high frequency

Never disable automatic updating!

2. Websites

People need to read the news on the Internet and be informed. The danger is that most office employees:

- browse the Internet from their office computers, running programs that may have vulnerabilities;
- perform their tasks under an administrator account in Windows;
- use weak passwords, which can be easily cracked;
- do not install security updates for the programs they use.

Uncontrolled web-surfing increases the risk of data leakage and unauthorised data modification.

Carberp family Trojans penetrate a computer ***while the user is browsing a compromised site.***
No action needs to be taken for the system to get infected. ***Infection occurs automatically.***

Websites that are more likely to be sources of malware (in descending order of incident frequency)

- Technology and telecommunications websites;
- Business websites: business outlets, business news portals, accounting-related sites and forums, online courses/lectures, and services for improving business efficiency;
- Adult content websites.

3. Removable media

Email is no longer the main source of infection even in highly protected environments. It has been superseded by removable media, particularly by flash drives.

IMPORTANT!

Removable media includes not only flash drives but also any ***USB device!*** *A virus can be transmitted* ***from one PC to another even with a camera or a portable media player.***

Trojans are today's most common threats. They are malicious programs incapable of self-replication and usually spread from one machine to another via user-owned flash drives.

4. Employee personal devices (including handhelds)

More than 60% of employees remotely access a corporate network from their personal devices, including their handhelds.

People don't just work in offices; they work while commuting and while at home. They often sacrifice hours of rest while staying connected. Businesses willingly takes advantage of this approach. In many companies, people never step foot in the office and access the network remotely.

But every coin has two sides. In other words, everything has a downside. In yesterday's world, such an approach guaranteed the desired level of security since system administrators controlled every single device at a company's disposal. But now that's impossible.

Threats

- Office computers are no longer the only targets of cyberattacks—personal devices (including handhelds) are at risk too.
- Almost two-thirds of employees (63.3%) remotely access a corporate network from their personal devices, including their mobile phones.
- Up to 70% of infections get into a corporate environment from personal laptops, netbooks, ultrabooks, mobile devices, and removable media (flash drives), which are often brought from home.
- Around 60% of home computers have no anti-virus protection! So outside of their offices, people are working with devices that are prone to be compromised by hackers; the applications they use may have vulnerabilities and their computers can be infested with viruses and Trojans. And yet these people regularly access their company network.
- This greatly increases the risk of data leaks and unauthorised data modification.

Facts

- A company's employees may be good professionals, but they aren't experts in anti-virus protection and often buy into misinformation.

5. Email

Mail traffic is the main transport for viruses and spam. If malware infects a computer, it can access an employee's address book which, along with the contacts of other employees, may contain the addresses of customers and partners—that is, any infection won't be confined to the corporate network but will spread beyond it.

Carelessness, negligence, and ignorance of the simple basics of computer security are often reasons computers become ensnared in botnets and sources of spam. This damages a company's image and can get it on a blacklist and force its provider to disconnect it from the Internet for sending out spam

6. Social engineering techniques Social engineering techniques

Most modern malware found in the wild can't spread on its own and is meant to be distributed by users.

It is users, ignorant of computer security basics or simply tired or careless, who unintentionally help malware penetrate a network (by using USB devices, opening emails from unknown senders, and surfing the Web during working hours).

To distribute Trojan programs, virus writers resort to social engineering techniques to take advantage of users and trick them into launching malicious files. They can send users phishing links, bogus emails from banks or social networking website administrators, and much more. The aim of all social engineering techniques is to acquire personal information, ranging from passwords used to access various web services to confidential and bank account information.

III. Company tasks. Actual tasks in relation to the structure of a corporate network

During a typical work day, a company's employees:

- create text and image files on computers and mobile devices;
- send and receive messages both inside the company and to/from external addressees;
- receive, send, and facilitate the receipt of data from the Internet—usually in the form of files;
- store or download information from company file storage, including information in the form of files.
- It's hard to find organisations where employees are not involved in activities like these. Therefore, in most cases, companies know that certain tasks must be performed in order for an anti-virus protection system to be established. The only question is: how many employees are to be involved in performing those tasks?

For a company's tasks to be performed, its local network should include:

- **workstations and/or terminal clients** (places where employees or visitors work);
- **file servers** for storing information, including files and documents, and for exchanging information between company employees;
- **database servers, application servers** (e.g., 1S server), **DNS/DHCP/Active Directory servers** – for everyday tasks, business procedures, organising network connections, etc.;
- **mail servers** for processing internal and external emails;
- **Internet gateways** for organising connections from the local company network to an external network (usually, but not always, the Internet).

Naturally, all these types of nodes are not always found on a network, and other types of nodes can be present, but in **most cases** a corporate network connects PCs and **at least** one mail server and one Internet gateway (for example, a PC is connected to an ISP's network).

There are very few exceptions:

- **All or a portion of the staff accesses the Internet via other networks.** In this case, there is no server or Internet gateway. This option is rather costly so companies rarely choose it. It can be adopted either by very small companies (e.g., notary offices) or by organisations where most of the staff works remotely. In such cases, the employees use public services.
- **The company uses external servers.** Companies usually hire email addresses or domains on an external server (e.g., on gmail.com).

Thus, usually it goes without saying that a company has servers. The question is

- how many servers does the company have—including those the company doesn't currently intend to protect;
- how compatible are their roles;
- where are they placed (locally or remotely);
- how do users access the servers (via the local network or remotely via the Internet), etc.

An ISP's local networks

Service provider networks (first and foremost ISPs) are unique in that they usually have two seemingly independent local networks. One of them is their local network. It has its own mail server, Internet gateway and employee machines. And the other is used to render services to customers. Thus for ISPs the common network includes:

- An Internet gateway for subscribers—users access Internet sites, external mail servers, and remote workplaces via the gateway.
- A mail server where customers can create their mailboxes or hire domains.
- The provider's internal network where the company's customers can place their own sites and store files, documents, etc. Typically, local traffic is free for customers.
- Virtual servers on which customers can run their own servers.
- The PCs and/or terminal clients of the ISP's employees.
- The provider's internal mail server — possibly (optional) connected to the server used to render services to customers.

Large providers can maintain a significant number of servers. This can be necessary for load-balancing purposes during peak periods and for backing up data in the event one or more servers fail. The availability or absence of certain types of components and the number of servers depend on a company's size and what kinds of services it renders.

ISPs can protect their subscribers from viruses and spam by:

- installing anti-virus and anti-spam agents on their customers' computers;
- scanning the clients' email and Internet traffic.

We recommend that you use those two methods to exploit the advantages provided by each of them:

- when traffic is scanned on a provider's server, user PCs have a reduced workload because they are not having to filter large quantities of spam.
- when anti-virus software is used on user PCs, malware will be prevented from entering via removable media.

Special systems

Some companies and organisations use systems designed to provide anti-virus protection in a special way.

These include:

High-load systems

With high-load systems, all or almost all hardware capabilities are utilised.

In ordinary offices machines involved in construction or design computing can serve as an example of such systems.

All anti-virus components, except for the file monitor, can be installed on machines like these.

Because this configuration does not provide resident security, it is recommended to allow archives to be scanned as they are being received and to conduct frequent (at least weekly, e.g., during weekends) anti-virus scanning.

The anti-virus engine incorporated into Doctor Web's software consumes very little of the available resources and can automatically reduce its process priority if the system is highly loaded.

Real-time systems

The specific features of real-time systems include:

1. A guaranteed execution time for each operation in a sequence—a cyclogram. Such systems are involved in engineered processes (fuel filling at petrol stations or in oil depots) or military activities (launching rockets).

   As you know, anti-viruses do not have scan time constraints. The average scan time can vary and change at least after every update.

   So, a fully functional anti-virus can't be installed in real-time systems.
2. Systems like these use special editions of common operating systems such as Windows NT4 and Windows Embedded as well as specifically designed operating systems such as Neitrino.

Anti-viruses are not compatible with such special platforms.

To protect real-time systems utilising common operating systems, you can install the anti-virus scanner which can be scheduled to check the entire system at startup. In addition, a real-time system must be used as part of a local network in which inbound traffic is scanned before it reaches the target host.

IV. The structure of a local network

The local network structure can appear as follows depending on what tasks a company needs to perform:

- **Computers, not connected to each other and with no Internet connection.** This structure is typically used in organisations where employees undertake work requiring a high-level of security. In this case, some computers or servers are excluded from the network, and data transfer between these computers and the network is performed with special (often registered) media. In particular, the allocation of the computers can be justified in the case of the need to reduce the security level and hence the level of the cost of its maintenance under the Federal Law «On Personal Data» No.152-FZ.
- **Computers, not connected to each other but with an Internet connection.** This variant is fairly uncommon. This structure is good for people who work remotely from home or do outsourcing. Each of these employees connects to the Internet, and the data exchange is provided via the network.
- **Computers joined to a local network and with no Internet connection.** This structure is typically used in networks with high security requirements. In such organisations, a network or computer is connected to the Internet, and the internal network is disconnected from the Internet. Special (often registered) media is used to transfer data between the internal and external networks.
- **Computers with local network and Internet connections.** This is the most popular structure and it doesn't require any additional commentary

If Internet access is available, information can be stored on PCs and local and remote servers, including those hosted in data centers (cloud services).

In addition to the network topology, user computer access should be taken into consideration. Two types of access exist—**single-user** and **multi-user.** Single-user access means that only one user can work on a computer; the second type of access means that multiple users are involved. As a rule, besides the user, a system administrator has access to the computer, which is why all these networks can be considered multi-user by default.

At the moment, multi-user networks are built on the basis of either work groups or domains. Other variants (peer-to-peer and networks based on Novell Netware) are less popular. The difference between work groups and domains is that the domain environment has a domain server (at least one or two—a primary server and a back-up server) that stores—in Active Directory—information about the network's users and computers, group policies and passwords, etc.

Information about the network structure is quite important; if it lacks a domain structure, all the computers may have a single administrator password, and, in that case, deploying an anti-virus network will be more difficult.

The impact of legislation

The type of activities a company engages in can determine its network topology and its anti-virus system because legislation requirements for a particular type of activity can force some companies to make adjustments. For example, a company may be involved in storing or processing classified information or cooperate with other institutions that have access to secret information (e.g., the Ministry of Defence or companies engaged in military research and development projects).

In addition, an organisation may be responsible for maintaining critical infrastructures (railroad communications, nuclear power plants, etc.), and thus be subject to the requirements imposed on companies that protect critical infrastructures. Typically, such companies isolate their local network from their external network. And most of the employees should not have Internet access or only have access to certain services.

Clouds and LANs

As a rule, a transfer to the cloud means that PCs and servers are transferred to a data center or that external services are used instead of those that may be available in a local network.

This lets you reduce infrastructure maintenance costs and increase the fault tolerance of server subsystems, but at the same time security risks increase:

- criminals and malware can access corporate data on remote servers (a contractor's employees can be involved; malware can easily penetrate unprotected virtual machines),
- information can be intercepted and modified when it's being transferred to remote servers,
- remote servers can fail or the connection can be lost.
- Switching to external services involves new security risks:
- data-transfer security costs increase when a protected data channel is organised; requirements increase for channel capacity, money needs to go towards purchasing related products, and licenses need to be acquired in order to work with encryption tools.
- there is no guarantee your service provider's staff won't be able to access your information.
- data transferred to a cloud can be hard to remove.

And this is not a full list.

Similar problems arise when employees use third-party cloud services since data from the cloud is transmitted over a secure channel that bypasses security systems, which means any data can be transferred by users.

By transferring its services to a cloud, a company relinquishes control over its information security and entrusts it to their service provider.

Cloud anti-viruses are another popular trend. Typically, data centers facilitate their services by means of VmWare products. To maintain anti-virus security, each data center server runs a special virtual machine that relays all the traffic and where all the file operations performed on the data center's other virtual machines are monitored by the anti-virus—the other virtual machines do not run anti-virus software. This approach to anti-virus security is based on the false assumption that anti-viruses detect all the malware trying to penetrate the system and disregards the fact that previously unknown malicious programs can avoid being detected by anti-viruses. In addition, this protection scheme is contrary to developing safety standards—native standards «Information protection. Information security with virtualisation technology». In particular, according to this document the following is required:

- scanning for malware in the boot areas of machine-readable medium, connected to IC;
- scanning for malware in firmware, physical and virtual hardware;
- scanning for malware in the memory and the hypervisor file system and (or) in virtual machines;
- scanning for malware in image files of the virtualised software and virtual workstations, machines, and in image files used for the operation of virtual file systems;
- scanning for malware in hypervisor configuration files and (or) in virtual workstations;
- network traffic filtering in the hypervisor's virtual networks;
- network traffic filtering for each virtual workstation;
- network traffic filtering between virtual infrastructure components, between internal and external network nodes of the host OS (of the hypervisor), and when establishing a network exchange with networks such as the Internet;
- scanning the data storage system in the hypervisor's operating environment for malware.

All the aforementioned can only be implemented if anti-virus software is installed, including on each protected virtual machine.

In view of the above, when using cloud services, you must take into account measures that can prevent:

- unauthorised access to data stored on remote servers; theft and/or data tampering during the transfer of data between remote servers and between the servers and workstations in the company's local network.
- malware from penetrating remote servers during data transfers.
- downtimes when remote servers are unavailable.
- These measures are as follows:
- encryption and VPN tunnels.
- mail gateways on the data center's end and on the LAN's end, or local mail servers scanning incoming mail and accumulating email messages when the data center is unavailable.
- ile servers and services synchronising the content with the content of remote servers.

The Dr.Web Anti-virus service for business can serve as an example of such an external service. Instead of investing in their own anti-virus infrastructure, companies can utilise the resources of a service provider that has deployed the Dr.Web AV-Desk Internet service. Significantly this service has been designed to enable customers to maintain reliable anti-virus protection even when the anti-virus server is unavailable.

External services

Employees of companies and organisations often use free and paid cloud services—mail, document storage services, etc. (google .docs, google .mail, google .disk and such), the access to which is not controlled by company security systems.

Using these services also involves certain risks. External services offer malware convenient ways to infiltrate a company because there is no guarantee the documents stored on remote servers won't be tampered with. Consequently, modified files received from cloud services get into a local network. Since the data is transmitted over a secure channel, the files bypass established security mechanisms such as Internet gateway anti-virus solutions.

Thus, a company should protect all the nodes that may be involved in the storage or transmission of malignant files. These include at a minimum 1) workstations, 2) mail servers and Internet gateways.

V. Russian legislative requirements for the field of anti-virus security

At the moment, there are two documents (containing information security requirements) subject to compulsory implementation on the territory of the Russian Federation:

- the Federal Law «On Personal Data» No.152-FZ;
- the information security standard of the Bank of Russia («Standard of the Bank of Russia for providing information security to organisations from the Russian banking system-1.0–2010»).

And while the above-mentioned standard is mandatory only for the banking sector, Federal Law No.152-FZ is mandatory for all companies and organisations, regardless of the type of activity they engage in, and for individuals.

In addition, there exists the «Doctrine of Information Security of the Russian Federation» (http:// www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm), as well as a number of other documents and standards, but they are either not mandatory or apply only to certain organisations.

In this regard, let's take a closer look at the requirements stipulated in «Standard of the Bank of Russia for providing information security» and Federal Law No.152-FZ.

The Federal Law «On Personal Data» No.152–FZ

Contrary to established opinion, the Federal Law «On Personal Data» No.152-FZ does not describe how an entire network is to be protected; it only describes how personal data processed on the workstations of selected networks is to be protected—the protection of other workstations and data transfer channels is not subject to this law. In this regard, it's generally possible to reduce the cost of a network protection system—data anonymisation or isolating data while it's being processed on selected workstations allows the law's requirements to be applied only to selected workstations, not the entire network.

The Federal Law «On Personal Data» No.152-FZ has almost no bearing on protection requirements—all the requirements are contained in regulatory documents (authorised federal bodies include the Federal Supervision Agency for Information Technologies and Mass Communications, the Federal Security Service, and the Federal Service for Technical and Export Control) and government decrees.

According to the law, personal data operators are all legal entities and natural individuals regardless of their form of ownership, size and type of activity.

The law and regulatory documents determine:

- who is a personal data operator;
- the rights and responsibilities of personal data operators;
- a regulatory list;
- the rules on personal data processing;
- the procedure for completing and submitting a notification on personal data processing;
- the types of control and the procedure held by the regulator;
- the list of documents to be created while provisions of the law are implemented;
- types of threats and the procedure that determines their importance;
- the information system classification procedure;
- personal data protection methods, depending on the system classification and actual threats.

The implementation of the Federal Law «On Personal Data» No.152-FZ in the field of anti-virus protection requires that:

- anti-virus protection be deployed on all servers and workstations where personal data is processed;
- the required level of access be given only to necessary resources;
- Internet access channels be protected;
- the protection is centrally managed.

Which implies:

- the use of centrally managed comprehensive protection on workstations and file servers; this includes anti-virus protection products and office control products **(Dr.Web Control Center + Dr.Web Desktop Security Suite Comprehensive protection + Dr.Web Server Security Suite);**
- centrally managed anti-virus protection for mail servers and Internet gateways **(Dr.Web Control Center + Dr.Web Mail Security Suite + Dr.Web Gateway Security Suite).**

The information security standard of the Bank of Russia (Standard of the Bank of Russia for providing information security to organisations from the Russian banking system–1 .0–2010)

The banking sector is a strictly regulated area of responsibility.

In particular, a bank information security system must meet the requirements of the Information security standard of the Bank of Russia (Standard of the Bank of Russia for providing information security to organisations from the Russian banking system-1 .0-2010), the law on personal data, and other standards describing information security requirements (for example, national standard "□ □□□/□□□" 13569)

Operations with merchant cards are strictly regulated. Local networks of banking institutions have their own unique issues—banks have branches in hard-to-reach areas of the country and abroad, external devices (ATMs) are used, and employees and bank clients can access services remotely.

Currently the information security standard of the Bank of Russia (Standard of the Bank of Russia for providing information security to organisations from the Russian banking system-1 .0-2010):

- determines the terminology, the main threat models, and the aims of organisations to detect them;
- lists the main types of objects to be protected as well as access privileges and the roles of the employees having those privileges;
- gives guidance on network configuration;
- defines the requirements for anti-virus protection and the policy on how to use Internet resources at different stages of the network life cycle.

In accordance with the requirements of the standard, a portion of the software should be protected against:

- the intentional or unintentional disclosure, tampering or destruction of protected data. In particular, this implies the use of means that restrict access to various resources such as Office Control (Office Control is only available with **a Dr.Web Desktop Security Suite Comprehensive Protection license);**
- he installation of protection tools by anyone other than the administrator and prevents people from tampering with the protection system's operation or changing its features. This requirement leads to the need to control the access rights to system settings and protect them against tampering. This implies the use of software products in the network that support the role-based access principle and the use of Office Control features **(Dr.Web Control Center + Dr.Web Office Control,** which is only available with a **Dr.Web Desktop Security Suite Comprehensive Protection license).**

The anti-virus protection should be multi-layered, and protection tools should be installed on both workstations and servers **(Dr.Web Control Center + Dr.Web Desktop Security Suite Comprehensive protection + Dr.Web Server Security Suite).**

An organisation that meets the requirements of the standard should use only protected email. Together with the requirement to protect against viruses and spam, this implies the installation of anti-virus mail-filtering tools (an anti-spam is only available with a **Dr.Web Desktop Security Suite Comprehensive Protection license);** in accordance with the standard, all servers (including mail servers) should not be directly connect to the Internet; the anti-virus protection system can be divided into two parts—an anti-virus gateway that has Internet access or is moved to the perimeter network, and a mail service **(Dr.Web Control Center + Dr.Web Mail Security Suite + Dr.Web Gateway Security Suite).**

In turn, Internet access should be used only to ensure bank activity. This implies both the use of Office Control tools to limit the list of available resources (Office Control is available with the **Dr.Web Desktop Security Suite Comprehensive Protection license**) and the use of traffic scanning tools to prevent viruses from entering from available but compromised resources (SpIDer Gate HTTP monitor is available with the **Dr.Web Desktop Security Suite Comprehensive Protection** license). Additional requirement are as follows: protection against hackers, which at a minimum means having a reliable firewall (Dr.Web Firewall is a component of **Dr.Web Desktop Security Suite**).

All the protection tools an organisation uses should be purchased legally.

In summary, an anti-virus for the banking industry must:

- provide centralised network protection;
- support roles with different levels of available privileges—both administrators and common users;
- protect all network nodes—workstations and servers, regardless of what operating system is in use. The standard does not stipulate the protection requirements for external and embedded systems (including ATMs). However, logically speaking, those systems should also be protected against malicious objects that have been designed to penetrate them;
- use office control, a firewall and a traffic control system along with anti-virus protection;
- provide anti-virus protection for a local network that does not connect directly to the Internet; this includes the receipt and distribution of updates in such a network and moving some services to a perimeter network.

It is recommended that the provisions of this standard and other standards be enforced, but in fact, banks are certified on the basis of these standards.

Find more detailed information on the Standard's requirements at:

http://www.abiss.ru/doc.

VI. Errors made when implementing an anti-virus protection system for a local network

When companies are not aware of the most common ways malware infiltrates corporate networks, don't know about the state-of-the-art features available in today's anti-virus solutions, lack knowledge of the legal requirements involved in protecting local networks, and employ IT professionals who hold certain misconceptions, widespread mistakes occur when they go to deploy an anti-virus protection system for their local networks.

1. «The fact that we protect our PCs is enough. There is no need to protect our servers»

It's typical for most companies to use only an anti-virus to protect their local networks. Such companies also believe that:

- It's pointless to protect servers because viruses can only gain entry through workstations;
- All incoming files pass through PCs, and protecting those PCs is sufficient; the anti-virus installed on PCs must detect and remove all the malware getting into the corporate network;
- No one works on servers and, therefore, no one can infect them;
- Server protection is expensive.

As a result, the deployed anti-virus protection system does not provide even the minimum required security level.

- Reasons why you need to protect your servers (file, terminal, application servers (databases)):
- A server may be infected with a virus that was **unknown** at the moment of infection and which first penetrated a user's computer and then spread across the network. An anti-virus running on the server will detect it with its heuristic routines. Or it will at least cure the virus after the next update occurs. A server that is not protected with an anti-virus will be a constant source of infection.
- A server can be hacked. An anti-virus installed on a server will detect and destroy malicious programs. If a server is running under a centralised control system, the administrator will be notified immediately when a workstation status has been changed (for example, when someone attempts to shut down the protection system).
- Users may work not only in the office but also at home; they may store data on their company's file servers and on Internet file servers; they may use their own flash drives—or those of their colleagues and friends. These media can be compromised with viruses. Modern cell phones already have the same features and vulnerabilities that PCs have. They run OS and use applications that may also be compromised. From these devices, viruses can penetrate a corporate network and access its server.

2. «A company must only protect its own devices»

No one has ever denied that it is imperative for an enterprise to protect its workstations. But the most common mistake companies make when deploying local network protection is to decide to protect only their employees' office computers.

In yesterday's world, such an approach guaranteed the desired level of security since system administrators controlled every single device at the company's disposal.

Now that's impossible—today a large portion of computers found within a company's premises don't belong to the company. These are their employees' laptops and smart phones.

Up to 60% of employee personal devices and home computers are left unprotected.

Their employees often access the corporate network from these computers that can serve as a springboard for hackers to penetrate the local network and bypass all protection systems.

It is in a company's best interests to ensure the security of all the devices used by its staff, no matter where the devices are used or who owns them.

IMPORTANT!

Dr.Web Control Center facilitates protection management for office computers and home devices, including mobile devices running Android and Windows Mobile.

3. «An anti-virus alone is enough. Comprehensive protection is excessive»

To protect their workstations, most companies settle on the purchase of just an anti-virus, passing over products that provide comprehensive protection. They believe an anti-virus is sufficient and that even if a workstation gets infected, the anti-virus will neutralise the virus and they'll have little spam.

In this case, it is falsely assumed that **the anti-virus's only task is to prevent malware from penetrating the local network**—in other words, it is believed that a high-quality anti-virus needs to recognise all or most malicious programs at the time of penetration. Dr.Web CureIt! is responsible for neutralising active malware programs that have already penetrated a system (unfortunately, companies are using the free version of this license, which is illegal), and an anti-virus that fails to detect malware is considered to be of poor quality and deserving of replacement.

IMPORTANT!

Today's anti-virus solution is quite different from yesterday's file anti-virus.

An anti-virus can detect and destroy malicious files, but it can neutralise only those threats **known** to the virus database or threats that can be detected by heuristic mechanisms. Before being updated, an anti-virus cannot detect or neutralise a **new, unknown** threat.

Comprehensive protection can prohibit the use of removable media and restrict access to local devices, including local computer directories and websites, in order to prevent infection—a new virus, one that has not yet been analysed by an anti-virus laboratory and, therefore, not yet determined by any anti-virus to be a virus will simply not be able to get on a secure server or workstation.

The benefits of comprehensive protection

- Internet traffic is scanned before being processed by a browser and mail traffic is scanned before being processed by an email client. This means that viruses won't be able to take advantage of vulnerabilities in the relevant programs; for a long time, software vulnerabilities (especially those in Adobe Systems software), rather than operating system vulnerabilities, have been mainly used to penetrate computers.
- The amount of spam in email traffic is reduced to a minimum, which significantly increases productivity because:
- Users are much less distracted from their tasks by incoming emails;
- Important messages are less likely to be skipped or deleted.

«All threats come from the Internet. Why should I protect a computer if it is not connected to the Internet?»

Some people think that a computer with no Internet or local network connectivity can go unprotected. These unprotected computers can be considered security holes in a company's protection system because hackers can use them to compromise local networks.

The main way malware penetrates local network computers or customer computers is through the removable media that employees are able to use freely when Office Control, which has an access differentiation system, is not installed on a computer.

5. «Viruses don't exist for Macs or Linux-running systems».

Another misconception is that fewer malicious programs exist for Mac, Linux and Unix operating systems, and thus only workstations and servers under the Windows OS need protection. Consequently malicious programs get a kind of asylum on unprotected computers—even if they can't infect these operating systems and running applications, they can use them as a source of infection—for example, using shared network resources.

IMPORTANT!

In 2013 the quantity of attacks on Linux rose dramatically. If news about Linux infections were rare in the past, by mid-2013, information about a new mass infection or hacking was appearing almost weekly.

6. «Emails are not opened on the server, so the server won't get infected. And our system administrators are professionals—they'll never allow viruses to enter the network»

That's true, but if email is stored on the server, only an anti-virus for mail servers is able to remove malware from mailboxes.

In addition, it should be remembered that although anti-viruses for gateways and email systems intercept viruses at the stage of their distribution (penetration) and do not play a role in protecting against malicious programs at the stage of activation (launching)—this happens on PCs—an anti-virus must be used to protect the file system in addition to the protection installed for services running on servers (including the mail server).

7. «The Anti-virus Control Center is only needed to make things convenient for system administrators»

This is a misconception. Companies that employ an anti-virus protection control center significantly impact their level of information security. The Control Center **guarantees compliance with information security policy** on all protected hosts. The Control Center makes it possible to:

- create individual settings for different user groups; the settings can be specified without having to configure the protection components on each workstation;
- guarantee that the anti-virus on each workstation is not disabled and works with settings established by the network administrator;
- regularly update the system and scan computers.

IMPORTANT!

The Dr.Web Control Center is provided free of charge.

VII. General requirements for implementing an anti-virus protection system for a local network

1. An anti-virus protection system should:

- have a persistent self-defence mechanism that prevents unknown malware from disrupting the operation of the anti-virus and ensures the anti-virus protection system is operational before it receives an update that will enable it to neutralise a threat;
- have an updating system that is controlled by the anti-virus's self-defence system and that does not use the components of the operating system, which can be compromised; have an updating system that upon receiving a signal from the centralised control system can immediately deliver updates so the anti-virus can cure an active infection on the object it is protecting;
- have routines for collecting information about new threats that make it possible to quickly send to the anti-virus laboratory the information needed to analyse viruses and release updates;
- be not only able to cure received (inactive) malware, but also cope with malignant programs that were previously unknown to the virus database and are now running in the system;
- have additional (other than signature-based and heuristic) routines to detect new, unknown malware;
- check all files entering the local network prior to their being processed by the respective applications. This rules out the possibility that malicious applications will exploit the unknown vulnerabilities within these applications;
- have routines for the centralised collection of information from remote PCs and servers, which will allow all the information needed to solve a problem to be quickly transmitted to the anti-virus laboratory;
- have a local support service in English.

1. An anti-virus protection system should:

- ensure the fastest possible delivery of the virus database updates for all the protected PCs and servers; this includes delivering updates on demand even if the protected network's overall performance is negatively impacted. A constant connection between the protected hosts and the updating server and the small size of the updates will minimise the update retrieval time;
- prevent users from disabling updates. The opinions of employees—regardless of their position—should be IGNORED when it comes to how frequently updates are applied.

IMPORTANT!

No other software requires such frequent updating as an anti-virus. New viruses are constantly being written, and the virus databases are updated at a very high frequency (at least 1–2 times per hour). Automatic updates should never be disabled!

With the Dr.Web anti-virus protection system's centralised control, a user can:

- prevent employees from disabling critical updates;
- disconnect a non-updated agent from the network and, therefore, prevent epidemics from spreading in the local network and beyond;
- set the desired updating mode for Dr.Web components on protected workstations distributing the load at different time intervals;
- monitor virus databases and workstation statuses.

- prevent users from disabling regular scans, start uninterruptible scans, and set scan schedules at any desired frequency. The opinions of employees—regardless of their position—should be IGNORED when it comes to how frequently updates are applied.

WHY IS REGULAR SCANNING IMPORTANT?

An anti-virus is not aware of 100% of the viruses in existence at any point in time.

It may take days or even months after a new virus appears before its signature gets added to the virus database.

Even if the signature entered in the database is able to detect the virus, that doesn't mean it will be able to cure the virus—a lot of time may be needed to develop the cure.

Facts

- After the next update is applied, scanning may reveal a considerable amount of previously unknown anti-virus threats.

The scanner performs a deeper check than the one carried out by the file monitor, which is why the scanner sometimes detects viruses the file monitor could not — this is a natural phenomenon.

Protecting a local network using cloud services

Particular attention should be paid to protecting a local network through the use of cloud services. Using cloud services involves the following risks:

1. Data can be intercepted and modified during transfer. To minimise this risk, use proxy servers at the server end as well as at the customer end. Secure channels can also help, but it should be noted that malware can still intercept data when it is being transferred from the secure channel to the recipient application.
2. Malware can penetrate virtual machines. So all virtual machines should be protected with an anti-virus, regardless of their location.

Additional requirements

The following measures should be taken in addition to an anti-virus:

1. A company's internal network should be insulated from the Internet—the network should be divided into an intranet and an extranet.
2. User and administrator actions must be logged.
3. Important information must be backed up regularly.

The following routines should also be introduced:

1. Regular control over all information security mechanisms, implemented with the help of firmware.
2. Restoring operation of all information security mechanisms, implemented with the help of firmware.
3. Information security incident response procedures.
4. Notifications for employees and customers about information security incidents.

VIII. A description of network hosts and principles of protecting them

1. Workstations and mobile devices

Experience shows that PCs (including handhelds) and servers are the most vulnerable nodes on a LAN. From them viruses, and often spam, are spread. There are many ways for viruses to get onto the machines from which they spread all over a network—for more information, please refer to the section «Points of intrusion in a corporate network».

Protection for corporate workstations

1. Theoretically any error (vulnerability) in program code can be exploited to harm a system. The result can be a short-term failure as well as serious data corruption. Following these simple rules will help you avoid such incidents:
   - Download and install timely updates and new versions of all the software installed on your computer—not just operating system updates. For this, all the software must be acquired legally.
   - A centralised updating system should be used for all the applications installed on a PC. This will help the system administrator ensure that no known vulnerabilities are found on the protected machines.

   Only a competent system administrator can make decisions related to updating an anti-virus, installing software, or restarting a system in order to apply a security update for a program installed on a computer. Opinions of other users should be IGNORED, regardless of their position.
2. Centralised control should be maintained over all the anti-virus components on all the PCs on the network.
3. You also need to use the latest version of your anti-virus software.
4. All users, regardless of their position, should work only under accounts with limited privileges. The guest account should be disabled.
5. The system administrator should know about all the programs installed on the computers.
6. Users should not be allowed to install any programs. This prevents malware from bypassing the security system and getting installed on a computer.
7. Users should only be able to access resources they really need for their work. This requires configured control system and access restrictions to be used.

Dr.Web Office Control prohibits the use of removable media (such as flash drives) and restricts access to local devices, including local computer directories and websites, in order to prevent infection.

8. Email traffic should be scanned before messages are downloaded by a mail client to prevent malware from successfully exploiting its vulnerabilities.
9. Internet traffic should be scanned before applications process it. The anti-virus should scan all download links and all traffic before it reaches a computer.

The SpIDer Gate HTTP monitor scans traffic before it is processed by a browser or a mail client. That way viruses won't be able to exploit vulnerabilities in programs installed on a PC.

10. Employees should have access only to resources they require for their work. The opinions of employees, regardless of their position, should be IGNORED when it comes to deciding what resource is secure for visitation. Access to Internet resources that are not required for work should be centrally blocked.

With Dr.Web Office Control you can:

- restrict Internet access;
- create blacklists and whitelists of addresses to provide employees with access to the Internet resources they need for their work;
- completely block Internet access when essential (for example, on computers with accounting systems);
- prevent employees from removing restrictions locally.

IMPORTANT!

- This component must also be installed on computers that are not connected to the Internet or are isolated from the local network.

11. Users (hence, malicious programs acting on their behalf) should only have access to the local resources they need to do their jobs. It's no use trying to convince employees that flash drives are dangerous.

Dr.Web Office Control's access restriction system:

- defines the local network files and folders to which employees can have access and those that are off-limits to them, i.e., it lets you protect data and sensitive information from being deliberately or unintentionally damaged, deleted, or held for ransom by attackers or insiders (employees seeking access to confidential information);
- restricts or completely prohibits users from accessing Internet resources and removable devices and, therefore, makes it impossible for viruses to invade via those sources.

An additional mechanism for protecting against viruses that spread through removable media is the blocking of autorun in SpIDer Guard. After enabling the «Block autorun from removable media» option, you can still use flash drives in situations when it is difficult to work without them.

Best practice

The ability to connect removable devices to a workstation should be centrally blocked.

12. In addition to an anti-virus, the following protection components should be used to protect a corporate network from being penetrated by malicious objects:
    - **Anti-spam** – reduces spam in mail traffic which mitigates the risk of infections resulting from spam messages and increases productivity.
    - **Firewall** – prevents a local network from being scanned from the outside and protects against attacks over the intranet.
13. Anti-virus software should be installed on all computers, regardless of their operating system– including Mac OS X, Linux, and Unix.

Protection for workstations involved in processing sensitive data or financial transactions

For these computers, there are a number of requirements in addition to the above.

1. A computer used for financial operations (online banking services) should not be used to work with critical data, and vice versa. No other operations should be performed on this dedicated computer.
2. The following restrictions must be imposed on the dedicated workstation:
   - disable other programs from being launched, especially those of unknown purpose and from unknown senders;
   - remove systems and services for remote control, and block features that facilitate a remote connection while business-critical systems are in operation—only allow access to resources used by the remote banking system;
   - use Dr.Web Office Control to disable access to other websites;
   - log all events, including all actions taken by administrators and users;
   - disable features allowing users to run programs from folders containing documents and directories containing temporary files, such as Temp;
   - use only strong passwords; a centralised security solution should ensure that only strong passwords are used and enforce regular password changes and security policy compliance.
3. Update the anti-virus and perform an express scan before starting to work with sensitive information and/or using online banking services.
4. When finished with an online banking session and/or working with sensitive data, users should log out of the system.

Protection for personal devices used by employees to access the corporate network

Nowadays many office workers use their own devices to access the corporate environment and/or work remotely. People in many spheres of employment stay connected wherever they are: at work, on the road, and at home. It's in a company's best interest to ensure their employees' devices are secure wherever they are and protect their corporate data.

Home computers usually run Windows. Because of this OS's popularity, hackers have studied it well—most malware targets Windows. Much work has also gone into studying how to best protect Windows, but with home computers accessing the corporate environment, a balance must be found between compliance with security policies and personal freedom. For example, access to social networks should be blocked during business hours and allowed in people's spare time. One must take into account that a home computer used by employees for work may also be used by other family members.

Two options are available in such cases.

- The first option is to add another user account on the home computer (since Windows features allow this) and adjust the account privileges in accordance with corporate security policy. Unfortunately, this method lets you fulfil only some security requirements. Even if working under a secure account will prevent infection, malware can still get in and access the unprotected data while other accounts are being used. Under an insecure account, it can also change the security settings. Therefore, protected data storage and integrity monitoring are necessary. But the main problem is that administrators will have to configure the software for each user, and, in most cases, they'll have to do it remotely.
- The second (more secure) option is to use a bootable disk or a USB flash drive containing all the components necessary for secure operation. Viruses targeting BIOS can bypass the defence, but those are still rare.

IMPORTANT!

Only by ensuring the security of all the devices used by their employees, including handhelds, can companies guarantee that the environment will remain malware-free and that passwords and other sensitive information won't be stolen.

1. An employee's opinion about what anti-virus should be installed on his/her personal device must be IGNORED until this device is incorporated into the corporate network. Otherwise, such a device should be declared «untrusted» and should not have network access.

2. The centralised anti-virus protection system should enforce an enterprise information security policy on the employees' personal devices, including making it impossible for them to disable updates and regular scans and remove certain protection components.

To close other security loopholes, deploy a solution similar to the system that will protect your corporate PCs.

Dr.Web anti-virus features allow you to:

centrally administer protection for your employees' work and personal computers and their mobile devices.

Protection for handhelds, including employee personal handhelds, that have corporate network access

Modern cell phones and mobile devices already have the same features and vulnerabilities PCs have. They run sophisticated OSs and use applications that can be compromised through the same methods criminals use to compromise computer applications. The main problem with employees using their own mobile devices is that malware can spread from them and infect a company's local network; in addition, malware can gain access to a local network's resources by bypassing protection.

The most common operating systems for handhelds are Apple iOS and Android and the latter's numerous modifications. Moreover, these operating systems feature resources that are less robust than those of workstation operating systems. These devices typically do not support multiple accounts, which would help restrict user privileges and reduce the risk of infection. Therefore, no all-round protection exists for them. In addition, there is a huge risk that a device will be lost or stolen and all the information on it (including logins and passwords used to access the corporate environment) will end up in the hands of a third party.

To prevent files containing malicious code from getting onto a device, the device should run:

1. **An anti-virus** – to detect malicious files designed to monitor user movements, contacts, and communications.
2. **Software that will allow a lost device to be found** or locked to prevent unauthorised individuals from accessing the information stored on the device.
3. **Software that protects classified information** in a secure storage to prevent criminals from accessing the information stored on the device.

Protection for mobile devices is mandatory if the devices are used to receive transaction confirmation SMS messages since some malicious programs can modify such messages.

2. Servers

As already mentioned, a typical «office» network may include:

- file servers;
- mail servers;
- Internet gateways;
- database servers, application servers, DNS/DHCP/Active Directory servers. . .

2.1. Combining server roles

Various server functions can be performed on the same machine or distributed between several server nodes; these nodes can be part of a company's infrastructure (and in this case the company is responsible for their security) or outside it (including in data centers).

In the first case, one machine can work as a file server, mail server, and Internet gateway. Therefore, when the functions of several servers are combined on a single server (not a virtualisation server – see below), we can speak about server roles—the role of a mail server, a gateway, and so on. We need to distinguish this combination of server roles from different servers launched via virtualisation systems. In the latter case, each server runs on a separate machine, isolated from other virtual machines, and does not affect other servers (if we don't take into account the use of a virtualisation server's resources).

Functions of different types of servers can be combined on a single server and if it is not a virtualisation server, we can speak about server roles.

Often one machine can simultaneously run an Internet gateway and a mail server. In addition to its main function (to store files and grant access to data), a file server can be used to establish other servers that maintain the network. For example:

- DNS/DHCP servers leasing local network addresses to a company's user machines;
- Active Directory servers storing information on network users;
- database and application servers (for example, a 1S server);
- terminal server;
- mail server;
- Internet gateway.

IMPORTANT!

- This role combination allows the number of company servers to be reduced (resulting in savings on server hardware), but it also significantly reduces the overall level of security because an intruder who cracks one server can access all the services installed on the company's network.
- With regards to network security and reliability, it is not recommended to run any other services, except a firewall, on the Internet gateway.
- It is also recommended to use a dedicated machine to run the AD domain controller.

If this combination is undesirable (because of security requirements, software incompatibility, etc.), one physical server can have several virtual servers that will separately provide multiple network services: DNS, DHCP, AD, file server, etc. In this case, when designing a protection system, one should take into account the risk of a virtual machine contracting an infection from a machine acting as a hypervisor as well as the risk of malware being distributed among the virtual machines.

The functions of different servers can be distributed among several servers. Such servers can be located either within a company's infrastructure (and in this case the company is responsible for their security) or somewhere else (e.g., in data centers).

2.2. Load redundancy and distribution redundancy

To increase the overall reliability of a server, redundancy of services is used—on both the server level (using failure-tolerant components, ride-arrays, etc.) and the service level; more servers than necessary are used to ensure a company's smooth operation, and if one server fails, the service isn't rendered non-operational. There are two types of redundancy:

- hot redundancy – when the load (e.g., inbound email traffic) is distributed among all the servers with the help of a load balancer. If one server fails, it simply won't be used by the system;
- cold redundancy – when a portion of servers is operating and the rest are standing by. If one operating server fails, the load will automatically be distributed on whichever server has been activated.

One service can be executed by several servers if one server clearly cannot cope with the load. If one server can't cope with the load, a load balancer is used, or the servers are united in a single cluster. In the latter case, the server is a cluster node.

2.3. File servers (a.k.a. database servers or application servers)

Functions and types of file servers

A file server is a computer on which user-accessible files are placed and stored.

It is important to understand the difference between file servers based on the Windows and Unix platforms.

Windows has a built-in file server function so that all users have shared access to folders (directories). The file server represents one server role, such as a DNS/DHCP server, an AD, a database server, a terminal service, a mail server, an Internet gateway, etc. But that does not mean a file server should be a database server or provide a terminal service—no role can be primary or secondary to another role. The administrator decides which role a server should perform.

IMPORTANT!

Under Windows, a file anti-virus scans all system files, not just shared files.

- In Linux, the file server functions are usually implemented through the optional installation of a Samba subsystem which emulates the corresponding Windows services.

IMPORTANT!

In Unix, a file anti-virus scans shared files only. This is because the file anti-virus for Unix is a plug-in (an additional module) for the Samba subsystem.

The number of file servers within a company

We can assume that every company has at least one Active Directory or DNS/DHCP server. Or even two—a primary one and a redundant one—as this service is crucial for a company. Cases when addresses are specified manually can be ignored because only small businesses find such a method convenient.

We can also assume that every large company has a 1S server. Companies rarely use a different accounting program or a non-server version.

File server protection

1. Security requirements for file server protection are different for Windows and Unix. For Windows, a file anti-virus should be used to protect application servers and terminal servers. For Unix OS, for each service a special solution should be used.
2. To establish reliable server protection for an organisation, one should:
   - know what additional services the file server has;
   - understand the consequences of sharing services on one protected service and how these services will be protected in this case.

IMPORTANT!

Just because databases are located on a protected file server, it does not mean that the contents of the databases will be cured; for that you need to use special solutions.

3. Quite often, employees use remote storages in addition to a company file server. When using such storages there's no guarantee users will receive files that aren't infected with viruses—criminals can intercept a communication channel and substitute the transmitted information. Therefore, in addition to a file server and protection for shared network resources (e.g., shared folders), a company should have an anti-virus gateway that won't allow an infected file to be received or transmitted.

2.4. Print servers

Quite often file servers are used as print servers, which means they have services that allow documents to be sent and received over a special protocol. These servers require protection because:

- many malicious programs can compromise print servers;
- intruders can intercept information sent to a printer and print documents that are for internal use only.

IMPORTANT!

If a print server runs Linux, not only does the file service function of this server require protection (a Samba service); the server itself should also be protected. For this two Dr.Web products should be used:

1. Dr.Web Anti-virus for Linux
2. Dr.Web for Unix file servers

You need to take into account the risk of infection both for file servers and for printers, especially if they can be accessed via the Internet. A lack of available hardware resources on such devices prevents them from running anti-viruses. Therefore, access restriction should be used as a security measure.

2.5. Terminal servers

Their purpose and a brief description of their operation

If a terminal server is in use, items such as a keyboard, mouse and monitor are connected to the server directly.

Connectivity is achieved in two ways:

- a special device — a thin client which has no hard drive and is used only to connect to the terminal client.
- a special program for the operating system.

Terminal servers can be based both on Windows OS and on Unix OS.

Protection for terminal servers

A file system protection product for PCs may be used to secure terminal servers because the only difference between file servers and terminal servers in terms of protection is the fact for terminal servers, a check of the clients' terminal sessions (open or closed) is required.

- If only thin clients access the server, no thin client protection is required (no anti-virus software should be installed on thin clients). However, in addition to a **Dr.Web Server Security Suite license** for terminal server protection, a customer should purchase **Dr.Web Desktop Security Suite Comprehensive protection** licenses to protect terminal sessions. The number of licenses should be equal to the number of connections.
- If a terminal server is not accessed by thin clients, clients getting access to the server require protection (**Dr.Web Desktop Security Suite Comprehensive protection + Dr.Web Server Security Suite** should be purchased). In this case, the workstation protection system is the same (whether or not terminal server access is used). There is only one thing a customer should take into consideration: if workstations are used, the number of workstations is not equal to the number of terminal server connection licenses.

2.6. Virtual (including cloud) servers and workstations

Their purpose and a brief description of their operation

With the increasing capabilities of servers, it would seem advantageous to use the same server for organising operations for multiple services. However, combining services is often impossible or insecure. The use of virtual servers may be a solution. These servers have only one so-called hypervisor service. It runs operating systems in a virtual environment. These operating systems and their applications do not run on a physical server but on an emulated server.

3. Mail servers

A mail server is a service located on a standard file server.

The purpose of mail servers is

- to process incoming and outgoing mail,
- to execute mass mailings,
- to exchange data between company employees,
- to serve as the base upon which document flow systems are built.

The most common mail servers

- Microsoft Exchange, Kerio MailServer, Lotus Domino, and Communigate Pro are commercial solutions.
- Sendmail, Postfix, and Exim (only for Unix) are typically used only in free versions. If a company is small, its management is less easily persuaded that anti-virus protection is worth purchasing.

The number of mail servers in a company

All of a company's business processes depend on the flawless operation of its mail system and on that mail system being free of viruses and spam. Almost all companies have a mail server.

Companies seldom use external mail servers—even if a company uses cloud services, mail servers are usually administered by its employees or (if the services are outsourced) accessed by its employees. However, sometimes companies (usually small ones) hire mailboxes on public services (such as Gmail) instead of deploying mail servers of their own.

Depending on a company's size, it may maintain more than one mail server. In the case of a multi-branch network, each branch can have its own mail server which can be moved out of a company's internal network (into a demilitarised zone), etc.

Clouds and mail servers

Collocating a mail server in a data center improves its reliability. It now equals the reliability of the data center. However, on the other hand, any interruptions in communications with the data center (hardware failure or disconnection) result in the disruption of business routines for the entire company. Consequently, to avoid such failures, a company should employ at least two providers to maintain its mail servers and deploy backup servers in its network so that they can accept emails while the main server is unavailable. Using servers that ensure the integrity of email during its transfer will also be beneficial.

Establishing mail filtering

Mail traffic is the main transport for viruses and spam. If a company's network gets infected, the malicious programs on the victim's machine will have access to the address book in which both your colleagues' and your customers' addresses may be stored, and, thus, the company's email system could become a source of viruses and a way for viruses to invade all the network nodes.

- The presence of a large number of malicious files in mail traffic, and employee carelessness can cause:
- data losses and leaks caused by viruses and hacking tools;
- a local network to get hacked and made part of a botnet because of virus attacks;
- a company to get placed on a blacklist and disconnected from the Internet for sending out spam;
- a reduced response time for the mail server used to process spurious traffic;
- the mail server to perform poorly or crash;
- an increase in the internal network load and a decrease in the performance of network resources and channel bandwidth;
- server failure after a «mail bomb» is received;
- equipment downtimes;
- an increase in mail (including spam) storage costs;
- an increase in requirements related to mail server hardware, and therefore, the need to upgrade or purchase new workstations.

The company also suffers **reputational damage** caused by:

- the continuity of their business processes being breached;
- delays related to employment duties, or the inability to fulfil employment duties (downtimes);

- the probability of missing important information;
- lost work time spent on neutralising virus incidents;
- delays in the fulfilment of the company's obligations towards its customers and partners;
- an increase in the size of user mailboxes and their backups, which in turn leads to problems when searching for necessary information;
- consumers and partners feeling less confident in the company's abilities;
- the company starting to be perceived as technologically inept;
- the loss of customers or customers refusing to use the company's services.

1. It is necessary to filter both the company's external (incoming and outgoing) and internal mail—i.e., all of the ways mail is sent and received should be filtered.

If a company's network is infected, email can become a source of viruses that can penetrate all of the network's computers. This is because malicious programs on compromised workstations have access to employee address books.

2. Email should be filtered both on the server and on PCs.

This approach allows the workload of the mail server and PCs to be reduced significantly:

- Only a mail anti-virus can remove malware from mailboxes during regular scans—no other anti-virus can do this.
- Filtering email at the mail-server level not only increases filtering efficiency but also helps clean mail databases of previously unknown malware. This rules out the possibility that viruses will be accidentally sent to recipients. Server solutions for mail filtering installed on servers and gateways allow administrators to filter traffic according to specific data formats, file size limits and other criteria; such features are not available in solutions for workstations.
- The traffic is scanned before it is processed by the mail client. This prevents viruses from exploiting vulnerabilities in operating systems and related software.
- Filtering email at the server level rules out the situation when a user can disable the anti-virus or lower the level of protection—a company's management and system administrator can rest assured that the business environment is well protected.
- The protection is always up to date. Unlike PCs whose software can go without being updated for quite some time (e.g., during employee absences), server virus databases are always kept up to date.
- Conflicts between the anti-virus and other software (e.g., user-installed software) are decreased.
- Email, including spam, will be filtered on the server once, rather than several times on each PC—this will improve PC performance, and employees will be much less likely to complain about low PC performance and request your assistance.
- Thanks to anti-spam filtering, the mail server won't be involved in processing large volumes of spam (the amount of spam in email traffic reaches up to 98%, and filtering it out will improve the mail server's performance). This will reduce the number of complaints employees have about mail delivery delays and lost emails.
- The encryption and compression employed by server anti-virus solutions will help decrease local traffic; no other developer provides this feature in products for PCs.

3. A mail server must be protected

Protection for mail servers (for example, Dr.Web Server Security Suite) is obligatory in order to protect against viruses that are unknown to the anti-virus protection system at the time of infection. When unknown malware gets on a mail server and/or in mailboxes, it turns the mail server into a permanent source of malware.

4. All of the ways mail is sent and received should be protected (and not just the mail server).

The situation is unique with today's employees; they're using not only internal services but also external services, including mail services. Often employees responsible for ensuring the safety of a company are not aware such services are being used.

A company's possible mail flow scenarios

- Users (or programs they agreed to install without knowing their functionality) can send and receive messages:
- directly to Internet mail servers (via SMTP) if port 25 is open in the network;
- to mail services like mail.ru/gmail.com – via pop3/imap4 protocols.
- Users (or programs they agreed to install without knowing their functionality) can send messages over secure channels, and the server will not be able to check them.
- A server (or programs installed on it) can create its (their) own mailing lists and notify senders and recipients of various events independently.
- In this regard, it is necessary to scan the mail traffic that's not just running to the company's mail servers, but also the traffic that's running to external servers or uncontrolled companies whose level of protection is unknown. In practice, this means you should either:
- filter all corporate email on the mail server (using Dr.Web Mail Security Suite Anti-virus + Anti-spam) and additionally handle POP3 and IMAP4 on the Internet gateway (depending on the product processing traffic used on the gateway—Dr.Web Mail Security Suite Anti-virus + Anti-spam, Dr.Web Mail Security Suite Anti-virus + Anti-spam + SMTP proxy or Dr.Web Gateway Security Suite Anti-virus)—in addition to scanning email on workstations;
- filter all external email (POP3 and IMAP4, SMTP protocols) on the gateway (using Dr.Web Mail Security Suite Anti-virus + Anti-spam + SMTP proxy) and focus only on processing internal email on the mail server (Dr.Web Mail Security Suite Anti-virus + Anti-spam)—in addition to scanning email on workstations.

The second option is preferable since:

- the load on the mail server is reduced significantly (the amount of spam in email traffic reaches up to 98%, and its absence will improve the mail server's performance);
- the mail server is not directly accessible from the Internet so hackers cannot exploit vulnerabilities (both those previously known and zero-day vulnerabilities), including by means of specially compiled messages;
- the quality of filtering on a mail gateway is much higher due to the fact that the solution for a mail gateway is not limited by mail server features.

5. Email filtering must be comprehensive

Only comprehensive solutions for email that combine an anti-virus and an anti-spam can ensure its protection and reduce company's costs. Using an anti-virus without an anti-spam:

- allows criminals to carry out attacks on company mail servers and mail clients used by employees;
- increases traffic costs;
- increases unproductive, spurious loads on mail servers;
- reduces the performance of all employees who receive mail and have to clean their mailboxes of spam.

6. Additional security measures

- Quite often mail servers store users' email messages either permanently (users keep all their email on the company's server and get access to the IMAP4 protocol) or temporarily (until an employee returns to work). Since the chance always exists that **a new, unknown** virus will penetrate the mail before it (the virus) gets sent to the anti-virus laboratory, we recommend that you either regularly check users' mailboxes for previously undetected viruses or scan email before sending it to employees.
- If the premises of a company or organisation are not located within the same perimeter and are situated in several locations and a dedicated channel is used for communications between them, the delivery and sending of messages between the company's venues should be carried out through a gateway—even if the premises are located in the same building, the possibility always exists that traffic will be intercepted or tampered with.
- Email that has already been filtered should be moved to the quarantine and/or backed up to address any complaints about filtering errors (for example, if the detection level was increased above the recommended level). The quarantine and message backup feature of **Dr.Web Mail Security Suite** let you recover messages employees have accidentally deleted from their mailboxes, as well as conduct investigations related to information disclosure.

4. Mail gateways

A mail gateway—unlike a mail server—does not store emails; it processes them on-the-fly and passes them to their destination. Mail gateways are used by:

- **Access service providers** – for filtering out viruses and spam from customers' email.
- **Companies** – both to reduce the load on the company mail server and to isolate it from the Internet (enhanced protection level).

Mail gateways are used because they are efficient at filtering out malware and spam—this does not happen when filtering is implemented on mail servers. This is because of the restrictions mail servers impose on the operation of anti-virus software. For example, in the case of mail-traffic filtering for Microsoft Exchange, the API restrictions (the application programming interface for interaction between the mail server and the anti-virus and anti-spam filtering module) let you implement the scanning of only portions of emails (not the entire message) for malware and spam. In particular, this leads to the fact that the viewed statistics do not show the correct number of scanned messages since the plugin only knows how many parts of email letters have been scanned, not the actual number of email letters.

Since they have their own modules for sending and receiving email and accessing the Internet, mail gateways can implement filtering and authentication mechanisms that are not otherwise available.

IMPORTANT!

Companies using cloud-based mail services must take advantage of mail gateways—only this measure ensures that mail traffic is free from viruses and spam.

Types of mail gateways

Typically, mail gateways are based on Unix. Two types exist: one that uses a standard mail server (often a free one, such as Postfix or Sendmail) as a transit server, and one that uses a specific anti-virus solution containing a transit message module.

Less often, one of the MS Exchange Server roles (Edge) is used as a gateway. Essentially tasks (roles) performed by MS Exchange can be carried out on a single server or distributed across multiple servers. One of MS Exchange's roles is to serve as a mail gateway. However, due to the nature of the licensing, the division of roles requires the purchase of special licenses; thus, using **Dr.Web SMTP proxy** instead of Edge leads to savings.

Software solutions and appliances automatically filtering inbound and outbound traffic via all protocols can be used as mail getaways—including for filtering the email of employees who use external mail services.

IMPORTANT!

With regards to network security and reliability, it is not recommended to run other services, except a firewall, on the Internet gateway. It is also recommended to use a dedicated server to run the AD domain controller.

Principles of email filtering on the mail gateway

1. **Mail should be filtered via a mail gateway (Dr.Web Mail Security Suite Anti-virus + (Anti-spam) + SMTP proxy)**

   It is not secure to display a mail server on the Internet or in the internal network. An attacker has many opportunities to access the server, including by taking advantage of instrument bugs. Even if a company's premises are located in the same building, traffic can always be intercepted or tampered with.

   The best course of action is to locate the mail server on the edge of the network or in a specially organised demilitarised zone (DMZ) of transit (or Frontend) mail servers. The servers receive email and forward it to the main mail server inside the corporate network, simultaneously filtering traffic for spam and viruses before it reaches the company's internal network. These servers can be managed by both company specialists and third-party companies (e.g., data center specialists).

   It is strongly recommended that mail traffic be filtered on a gateway if a company:

   - is an Internet service provider;
   - has a mail server outside the protected area of the company (for example, in an external data center);
   - hires mail addresses via a special service;
   - has its premises situated not in one place but in several locations, and a dedicated channel is used to communicate between them (the company has a multi-branch structure).

IMPORTANT!

The anti-virus proxy server used in gateway anti-virus mail-filtering systems employs routines that significantly increase the quality of mail-filtering. These are routines that can't be implemented on a mail server due to the restrictions of the anti-virus's API used for server integration. For example, the anti-virus's API for MS Exchange does not allow it to receive whole messages, which significantly hampers the anti-spam analysis.

Gateway filtering advantages

- The mail server is not directly accessible from the Internet so hackers cannot exploit vulnerabilities (both those previously known and zero-day vulnerabilities), including by using specially compiled messages.
- Advantages of gateway anti-virus solutions (e.g., **Dr.Web Mail Security Suite Anti-virus + Anti-spam + SMTP proxy**):
  - they significantly increase network security;
  - they significantly improve the quality of filtering due to the absence of any mail server restrictions;
  - they decrease the workload for local mail servers and workstations;
  - they improve a mail-filtering system's stability.
- With email traffic processed by a gateway, spam doesn't reach the mail server. This dramatically reduces spam traffic and hence improves the mail server's performance and availability to users. As a result, IT infrastructure costs are reduced. These cost savings are achieved through:
  - a significant reduction in the cost of spam traffic;
  - eliminating the need to increase the number of servers or upgrade hardware;
  - a reduction in mail storage costs, including those pertaining to spam.

2. The server on which a mail gateway is deployed must be protected.

Like the mail server, the gateway is another service run on a standard server. Therefore, if a workstation runs Windows, you also need to protect the server in addition to protecting the mail gateway. In other words, you need two Dr.Web products instead of one: Dr.Web Server Security Suite and Dr.Web Mail Security Suite.

5. Internet gateways

Their purpose and a brief description of their operation

A server, via which users will be able to get outside the local network, is required since there are many Internet users and companies often have just one cable.

With gateway anti-virus solutions, you can:

- prevent malware from exploiting software vulnerabilities, including unknown ones, and, thus, reduce the risk of the local network getting infected and/or having its operation disrupted;
- accelerate workstation operation by transferring the company's anti-virus scanning solutions to the company's gateway.

Under a corporate policy, gateway anti-virus software typically allows access to web resources, as well as the policy for accessing certain types of files, to be controlled.

Software solutions and appliances that automatically filter incoming and outgoing Internet traffic via all primary protocols can be used as a gateway—including in cases when employees can freely access external Internet resources.

Every company with Internet access has an Internet getaway. Multi-branch companies have at least as many gateways as they have branches/offices.

Getaway security is necessary if a company has:

- servers located outside the protected area,
- branches,
- departments located at several addresses or separate premises.

IMPORTANT! If a company uses cloud services or has branches, gateways are obligatory—only they can ensure that traffic is free from viruses and spam.

Filtration principles of web traffic at the gateway

1. Typically, anti-virus solutions for Internet gateways are not independent programs—they are additional plugins for programs to be installed on the server and which provide Internet access.
2. Like a mail server, a gateway is another service run on a standard server. Therefore, if a workstation runs Windows, you also need to protect the server in addition to protecting the mail gateway. In other words, you need to purchase two products:
   - **Dr.Web Server Security Suite** (Dr.Web for Windows Servers)
   - **Dr.Web Gateway Security Suite** (Dr.Web for Internet gateways Kerio or Dr.Web for Microsoft ISA Server and Forefront TMG).

IMPORTANT! Without such protection, your corporate network can easily be compromised.

IX. Doctor Web virus-related computer incident (VCI) expert consultations

1. Cyber fraud and virus–related computer incidents

Definition

A virus-related computer incident (VCI) is a computer incident involving the use of malicious or potentially dangerous program(s).

Virus-related computer incidents prevail among the variety of information security incidents that occur. VCIs involve criminals employing malicious and potentially dangerous programs, as well as social engineering techniques, to make users launch malware or riskware. Such incidents are considered fraud, which means this segment of the information security service market can be referred to as **the cyber fraud incident management segment.**

The main vectors of commercial cyber fraud involve:

- Compromising computer systems—with a view to joining them together into botnets to spy on victims, steal information stored in a system, and organise denial of service (Dos) and distributed denial of service (DDoS) attacks.
- Stealing e-banking and online payment credentials to steal money.
- Stealing bank card data to steal money.
- Engaging in brand fraud for profit or, more rarely, for the purpose of discreditation.
- Stealing proprietary content.

Reasons why the number of thefts involving malicious software is increasing:

- the quantity of malware has increased,
- malware technologies have become more sophisticated,
- vulnerabilities that have yet to be closed by software developers are being exploited,
- victims are often using pirated software (including anti-viruses),
- security software (including anti-viruses) is being used improperly,
- Internet rules for safe behaviour are being violated (this includes the disabling of some anti-virus components),
- security settings (including those of the anti-virus) are configured incorrectly,
- basic rules of information security are being ignored,
- the human factor—negligence, carelessness, connivance, etc.

Cybercriminals are successfully exploiting the following to carry out attacks on corporate computer systems:

- downsides when the anti-virus protection systems of all the corporate network nodes are being deployed or when no anti-virus protection system is present (here, we are not talking about the use of anti-viruses; we are referring specifically to anti-virus protection systems);
- periods when a company's information security policies are being revised and periods when no information security policy is present;

- violations of information security policies by company employees due to their lack of knowledge of information security basics, lack of awareness about virus problems, and negligence;
- social engineering techniques.

IMPORTANT!

An anti-virus is the main method used to counter cyber fraud. Doctor Web develops effective and multi-purpose protection tools to combat programs used to commit computer crimes.

2. IT security response service

In 2013, Doctor Web expanded its scope of activity by offering information security and cyber fraud incident management services.

Today, Doctor Web has an information security incident response service. The service includes an expert computer laboratory that investigates artefacts related to security incidents, and an analytical team that compiles analytical reports and collects statistics.

3. VCI investigations

The investigation of software used to commit computer fraud is one of the procedural actions involved in cybercrime investigations; it is one of the most important elements of the evidence base.

Doctor Web investigates computer incidents committed using malware and potentially dangerous software to attack the confidentiality, integrity, and availability of computer data and systems.

Investigation request form: https://support.drweb.com/expertise.

Services provided with Doctor Web VCIs

- A preliminary estimate of the incident, the scope of the investigation, and the measures required to neutralise the incident's consequences.
- An examination of computer and other related artefacts (hard disks, and text, audio, photo, and video materials) presumably related to the VCI.
- Exclusive! A psychological evaluation of individuals (company personnel) to identify possible accomplices involved in/assisting with/covering up or supporting illegal activities against customers (a comprehensive risk assessment) and instances of inaction or dereliction of duty.
- Recommendations on the deployment of an anti-virus protection system that would prevent VCIs or reduce them to a minimum in the future.
- All the procedures are carried out in compliance with legislation of the respective country.

The advantages of Doctor Web VCIs

- Over 20 years of experience researching malware.
- A knowledge base of current virus threats, their continuous monitoring and analysis, unique detection methods.

- Effective at thwarting new threats; continuously improving technologies for neutralising new, unknown malware and criminal activities.
- Highly qualified personnel.
- Own global virus monitoring service.
- Own anti-virus laboratory.
- Exclusive! A unique investigation of customer personnel.
- Special equipment allows information to be retrieved in accordance with procedures that guarantee its complete retrieval and provide irrefutable evidence in court.

Hardware—subject to malware attacks examined by Doctor Web

- Server equipment;
- Payment terminals and ATMs;
- Staff desks equipped with desktops and laptops;
- Computers and mobile devices belonging to employees and used to connect to the corporate network;
- Any removable media.

The scope of an investigation, which determines what questions Doctor Web's investigation can help answer, depends on the amount of services the customer paid for when they concluded an agreement.

Questions	Answers
What was compromised (investigation object)?	▪ Whether the system's integrity was compromised. ▪ Whether the incident involved malware. (If it did, the incident is within the scope of a Doctor Web investigation). ▪ Whether the VCI was caused by deliberate actions.
Where did the VCI take place?	▪ The technical specifications of the system that experienced the VCI, and its environment. For what purposes the customer used the system (this information is necessary to determine the investigation's priorities). ▪ Whether the computer shows any signs of unauthorised access. ▪ Information about the security software installed on the workstation on which the incident took place and whether the software was compromised. If yes, a description of how the security software was compromised.
What caused the VCI?	▪ Staff violations of operational rules or security policies.
How did the VCI occur?	▪ Viruses and other malware involved in the VCI, including a description of their features and payload (those used in the incident as well as potentially dangerous ones). ▪ Steps taken by the customer's employees to discover the incident and after it was detected. An evaluation of the employees' actions.

The people involved in the incident	▪ The people involved in the VCI (intentionally or due to negligence), and the extent of each individual's involvement.
Available evidence of the incident	▪ Whether the incident is the focus of an investigation by law enforcement agencies. Whether there is a possibility to appeal to law enforcement agencies and subsequently seek legal redress. The chances to win the case. ▪ The list of collected evidence.
Measures to prevent similar incidents in the future	▪ Recommendations on the deployment of an anti-virus solution that would prevent VCIs or reduce them to a minimum in the future.

X. Rules of conduct after a VCI

Money stolen from online banking systems

Unfortunately, victims discover they've been robbed only after the fact. At this point, the way victims respond to the incident becomes extremely important. Before you follow our recommendations, make sure that the theft occurred as a direct result of a virus. For this purpose, it's enough to briefly interview the employees who have access to the e-banking system. If you or they did not perform an operation that you consider to be suspicious, a virus or an attacker is likely involved.

IMPORTANT!

- Do not attempt to update the anti-virus or run a scan—you may destroy the traces of intruders in the system!
- Do not attempt to reinstall the operating system!
- D not attempt to remove any files or programs from the disk!
- Never use a computer from which e-banking system authentication credentials have allegedly leaked, even if there is an urgent need to do so!

Your actions must be swift and decisive:

1. Immediately contact your bank; it may still be possible to cancel the transaction. Even if the payment has already been transferred, request that the bank block all transactions within the compromised account before issuing you new access authentication credentials (login and password, etoken, etc.).
2. Notify your bank (the one that sent the payment) by fax. Print out the request in TRIPLICATE and submit all three copies to the bank. Ask for the registration numbers to be included on two of the copies: one will remain with you, and the other will be attached to your statement to the authorities. Your application should contain the date and serial reference number of the document accepted by the bank secretary.

Sample application

3. Fax a notification to the beneficiary, the bank that received the funds from your account. Similarly, make THREE copies and register them.

Sample application

4. Submit a statement to the police and attach to it the two notifications for the banks (recipient and sender of the payment). To do this, visit the nearest police station.

Sample application

IMPORTANT!

We strongly recommend that you go to the police. A criminal offence has been committed against you.
Law enforcement authorities need your formal complaint (i.e., a legal reason) to initiate a criminal case against the intruders.

Sample application
If your request for assistance is refused, obtain a written waiver and forward your complaint to a higher police authority—the chief of police in your place of residence. Confirmation that an incident of theft has occurred is sufficient grounds for a criminal investigation.

5. Notify your provider in writing, asking them to provide logs of network connections for the period when the theft occurred.

Sample application

IMPORTANT!

ISPs keep logs of network connections for no longer than two days, so you don't have much time!

IMPORTANT!

Print all of the sample statements so that you have them at hand rather than on the Internet. Remember—the Internet may not be accessible at that exact moment.

All of the above must be completed within 1-2 days after the theft has been discovered!

Encoder Trojan encrypted files

Encoder Trojans are notorious for encrypting data on compromised computers. Such data can be recovered. Contact Doctor Web's technical support service as soon as possible!

IMPORTANT!

- Do not use the infected computer until you receive instructions from Doctor Web's technicians, even if you need it for your business.
- Do not attempt to reinstall the operating system!
- Do not attempt to remove any files or programs from the disk!
- If you initiated a virus scan, do not take any irreversible actions such as curing/removing the malware. Consult Doctor Web's specialists before you do anything with the found viruses/Trojans,
- or at least keep back-up copies of all the discovered malware; they may be necessary to determine the key to decrypting the data.

How to submit a request to Doctor Web's support service

1. Fill out the request form.
2. Provide as much information about the incident as possible, including the demands of the intruders. If you have an idea as to which file you opened to launch the Trojan, please attach the corresponding file(s) or link(s) to your support request.
3. Use the comment field of the request form to attach several encrypted files (if possible, different file types and sizes: JPG, ZIP, DOC, PDF, etc.) and the ransom demand text.

4. If the Trojan penetrated the system via email (such Trojans often arrive with notices ostensibly from banks) and you have not removed the email, save it into an EML file and attach the file to your request.

Submit decryption request

We strongly recommend that you file a report with the police.

A criminal offence has been committed against you.
Law enforcement authorities need your formal complaint (i.e., a legal reason) to initiate a criminal case against the perpetrators.

Sample application

Be prepared to have your computer temporarily removed for examination. If your request for assistance is refused, obtain a written waiver and forward your complaint to a higher police authority—the chief of police in your place of residence.

Blocker Trojan blocked access to Windows

IMPORTANT!

Under no circumstances should you pay the ransom—you will never get the promised unlock code from the extortionists.

Use Doctor Web's free service to unlock Windows when it has been disabled by a Trojan.

We strongly recommend that you file a report with the police.

A criminal offence has been committed against you. Law enforcement authorities need your formal complaint (i.e., a legal reason) to initiate a criminal case against the perpetrators.

Sample application

If your request for assistance is refused, obtain a written waiver and forward your complaint to a higher police authority—the chief of police in your place of residence.

3d street Yamskogo polya 2-12A, Moscow, Russia, 125040
Phone: +7 495 **789-45-87** (multichannel)
Fax: +7 495 **789-45-97**

www.drweb.com | www.av-desk.com | free.drweb.com