



Typical points of vulnerability in corporate IT security systems

July, 2011

Kaspersky Lab, a leading developer of secure content and threat management solutions, focuses on improving corporate customer experience and expanding the range of support services to business customers. As a part of this strategy, Kaspersky Lab established Global Emergency Response Team (GERT), the new division to offer consulting services for current and future corporate users worldwide. The goal of GERT is to help business customers to identify and mitigate security policy mistakes and malware-related outbreaks, perform forensic analysis and provide security policy consulting.

Within the last 12 months of active engagement with our corporate clients, we have noticed that the majority of malware-related incidents happens due to underestimated design issues or unnoticed weakness in security solutions or corporate security policies. We believe that it would be beneficial for Kaspersky Lab as well as our current and future clients to review common security issues and evaluate possible damage to corporate IT infrastructure.

This white paper is intended for corporate IT management and describes the most typical reasons for propagation of malware in the corporate network.

Contents

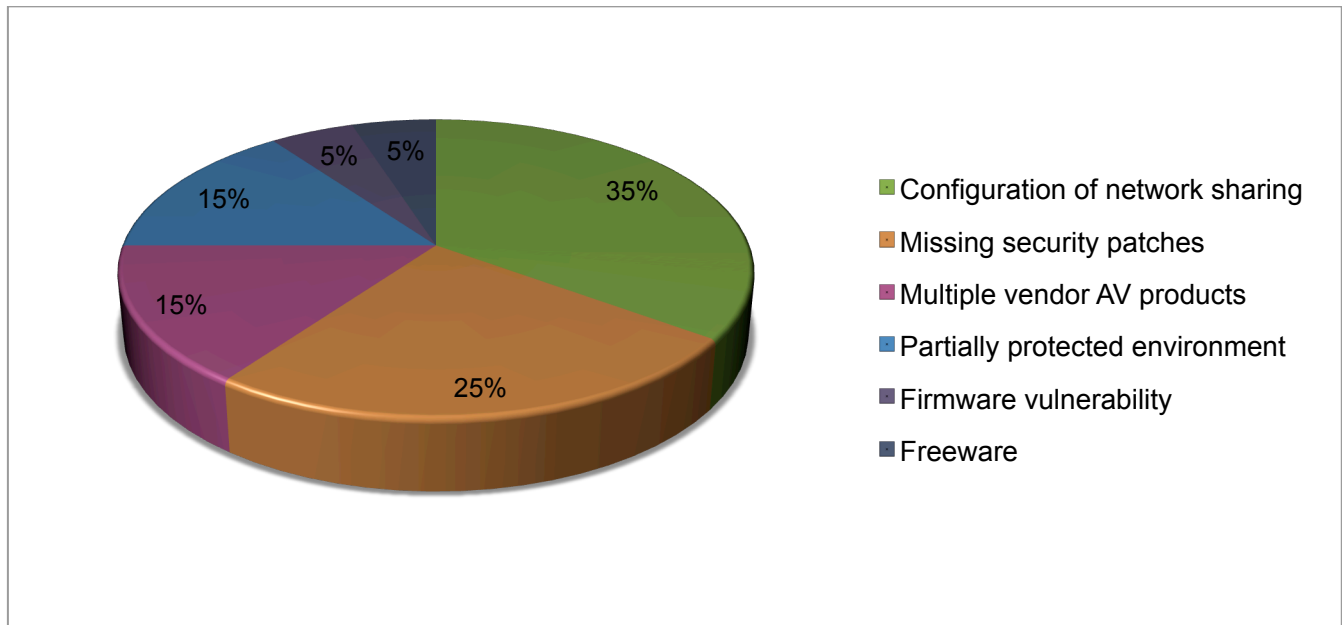
The most common security policy mistakes	3
Case study #1: Insecure public resources.....	3
How this case can be recognized.....	4
Mitigation steps	4
Case study #2: Delayed security patch updates	4
How this case can be recognized.....	4
Mitigation steps	5
Case study #3: Multiple AV products in the network	5
How this case can be recognized.....	5
Mitigation steps	5
Security advice	6
Case study #4: Working with offshore design teams.....	6
How this case can be recognized.....	6
Mitigation steps	6
Conclusion	7

[Toc298247131](#)

The most common security policy mistakes: overview

The statistics, gathered while serving corporate customers, Kaspersky Lab's Global Emergency Response Team uncovered the most common security policy mistakes.

Kaspersky Lab's Global Emergency Response Team experience in serving corporate customers helped to uncover the most typical security policy mistakes. Behind the numbers in this chart are the real-life incidents, involving malware infection and data loss. This statistics also shows, that the most common types of misconfigured security can be easily avoided, by following simple security rules.



This white paper describes the most notable examples of IT security weak spots, including:

- ▶ **Network file shares configuration.** Typically, no access control, full access to everyone, unnecessary write permissions to wide group.
- ▶ **Missing security updates** or outdated anti-virus database. Update schedule either not configured or configured to install updates too infrequently.
- ▶ **Multiple vendor anti-virus protection.**
- ▶ **Partially protected network environment.** AV solution installed only on some part of the network
- ▶ **Excluding non-executable files from regular system scans.** Non-executable files can also contain threats.
- ▶ **Vulnerability in firmware or settings of support devices (routers, Wi-Fi access points, etc.).** Default login credentials for these devices, no restrictions to access the devices from outside of the network perimeter.

For each case study the white paper also offers solution and security advice in order to avoid these kinds of internal vulnerabilities.

Case study #1: Insecure public resources

As an example for this scenario let's assume a typical City Public Library (CPL) that can be found in almost any town in the US. One of the most important missions for the library is to provide internet access and information exchange to visitors. In this environment we deal with inexperienced users and not much effort towards the security. Library visitors, using their own laptops or smartphones, are not required to use anti-virus software. The library desktops are usually not protected either, From the point of view of library IT staff, it is only necessary to offer protection for public file servers and private PCs.

What if some of the mobile resources are infected with an aggressive file infector, like the most recent Virus Win32.Sality? This virus propagates via open network shares and infects every file it can access. When running on

the infected mobile endpoint, Sality tries to infect all files on remote file share. The public file server becomes a perfect target.

In this environment, the server's anti-virus solution most likely detects Sality's malicious activity. The anti-virus repeatedly blocks remote attempts to modify files on the public share. These security events occur repeatedly in high volume because the AV product scans each file once all of its content is uploaded to file server. Finally, the public resource becomes unresponsive to normal users. The activity exhausts the server and network resources, in the same manner as the DDoS attack. The overwhelming load from the repeated attacks on the public shares will have similar result as disconnecting file server from the network.

How to recognize this case

- ▶ **End user complaints.** The end users report slow response from the remote file server or no response at all. If an anti-virus solution is installed, end-users may see frequent pop-ups alerting about malware attacks on their systems.
- ▶ **Huge volume of identical anti-virus notifications.** Typically, the IT personnel sees hundreds of alerts from the attacked server. Files are disinfected repeatedly. It might look like the server's AV scanner is unable to clean files, but in reality the file share is being infected over and over again.
- ▶ **Unusual network activity** to dedicated file server. You can see heavy traffic from multiple remote systems to the target host server.
- ▶ **There are many new or existing files in the shared directory and all of them have identical size.** Some malware may change the size of the files. For example, Sality changes file settings so the size of each infected file equals to 373Kb. This is very suspicious if hundreds of files in shared folder have identical size.

Mitigation steps

- ▶ Immediately isolate file server or stop sharing service on file server and start on-demand scan.
- ▶ Install an anti-virus product on all desktop systems and complete cleaning. To identify infected system see the anti-virus log. You can use Kaspersky Lab utility to clean network environment, available here <http://support.kaspersky.com/faq/?qid=208279710>.
- ▶ Set up the firewall and block infected laptop, phones from the network or limit their access to read-only to all public resources.
- ▶ You can also use offline anti-virus scanners, such as Kaspersky Lab's "Emergency offline scan" to mitigate malware effectively.

Case study #2: Delayed security patch updates

In some cases malware can take advantage of missing security patches. This can happen when the patch management process is not properly managed or the frequency of updates is too low. We have noticed that some corporate customers still do not pay attention to updating their systems with urgent updates.

A good example is a well known Windows OS vulnerability MS10-046 that was patched by Microsoft on August 2nd, 2010. This vulnerability was utilized by at least two viruses: Stuxnet and Sality. Stuxnet may infect end-user systems when someone inserts an infected external drive and Sality virus also propagates via open network file shares. New modification of Sality uses recent vulnerability in handling ".lnk" files as another method of propagation. We have seen it aggressively spreading using this exactly method.

This Sality variant consists of several files, with "autorun.inf" being one of the. This file is automatically executed when a new removable media is inserted into a computer. It contains a link to an infected dll file which is located on remote host. The remote host may be the system in the corporate network that was previously infected by Sality, or an external resource, like public file exchange internet resource.

You can read technical details of Sality .lnk exploit in details at <http://www.kaspersky.com/news?id=207576193>

How to recognize this case

-
- ▶ **End user complaints.** The end users may notice some strange network behavior or complain that operations with files take longer than before, or some network resources are not available, or frequent “file not found” errors and security alerts on their systems.
 - ▶ **Unusual traffic.** Network administrators can see spikes in network traffic between workstations. In particular, you can see high volume of peer-to-peer network connections for file downloads. Also, you can see high volume of file access failures.
 - ▶ **Repetitive AV alerts.** Some AV products may detect malicious payload (usually in *.dll files), but not the actual .lnk exploit. You can see frequent detection alerts on end-user systems that can be another sign of this problem.

Mitigation steps

- ▶ Initiate quick or full-scale anti-virus scan on all endpoints (laptops, workstations, servers, smartphones). Most anti-virus vendors distribute new signature updates soon after the new attack is discovered.
- ▶ Locate suspicious systems. You can do it by analyzing “workstation-to-workstation” and “workstation-to-file server” traffic. You need to identify those systems that attempt to access remote hosts for file-write or full access.
- ▶ Use the Kaspersky Lab Sality Killer tool. This is a powerful utility that finds and deletes all Sality variants. See details here: <http://support.kaspersky.com/viruses/solutions?qid=208279889>
- ▶ Temporary disable all file share servers and open file shares on workstations. You can re-enable all of them upon completing the cleaning procedure.

Case study #3: Multiple anti-virus products

Another potentially dangerous situation is mix of products from different anti-virus vendors. The common mistake is to believe that all vendors of security solution provide 100% protection against all malware. This is true for some vendors, but not for all. Let's assume there is a financial company called “My Best Bank” (MBB). The company has hundreds of branches across the country. Irrelevant of the office size they all run Windows workstations protected by antivirus product created by “Alfa-Antivirus”.

However, the core operations are done in main headquarters on servers with Novell Netware. This choice was made long time ago and the MBB is not going to change the software platform in the future. Those systems are protected by Kaspersky Anti-Virus for Novell Netware and are used to store important documents from local offices, headquarters and data backups.

The end-user in one of the offices decides to go to a software distribution website and download a program. When this program is launched, it is detected as suspicious by “Alfa-Antivirus” (that is protecting Windows-based workstations). The end user ignores this alert and downloads another version of the program from another website. This version is not detected by “Alfa-Antivirus” because it is obfuscated.

The malware successfully injects malicious code into Explorer.exe process and deletes itself from the file system. Few hours later a fresh version of malware is downloaded from remote website and successfully executed. “Alfa-Antivirus” stays green and calm. The infected endpoint quickly infects other user systems. During the next data backup the files are copied to Novell file servers where malicious files are detected by Kaspersky Antivirus. However, there is no any alert from Windows-based workstations. The systems administrator decides to initiate quick scan on all Windows-based stations, but nothing is reported by “Alfa-Antivirus”.

How this case can be recognized

- ▶ You can see detection alerts from anti-virus solution installed on file share server and nothing from anti-virus installed on workstations. In some cases an anti-virus may detect malware within last 3-4 days and then stop detecting it.

Mitigation steps

- ▶ Locate and isolate infected workstations. You can do it by examining file share detection log.

-
- ▶ Change workstations anti-virus solution while monitoring for other suspicious systems in the network.

Case study #4: Working with remote design teams

This case is related to security policy configuration that defines AV scanner configuration for portable media, like external USB devices, email attachments and other workgroup resources are verified. In some cases scan of non-executable files can be disabled for performance reasons. However, some malware can be written as non-executable files targeting particular products file formats, e.g. AutoCad files.

Let's assume there is a middle size company "Project Designer" that has remote developers. The remote team works on design of particular project component and sends AutoCAD drawings weekly to Head Quarter team. Then, HQ engineers copies drawings into common folder for shared use. The HQ team routinely checks incoming data for malware, but for performance reasons the scanning process includes only executable files.

The attacker can create malicious component that will run when AutoCAD loads an AutoList script. When executed, this script might create other malicious components, auto-startup services, download updates from the Web or to propagate to open network shares. A good example is Trojan.Acad.Dwgun. It comes to victim as the AutoCAD dwg file. Malicious function activates when someone opens it. Depending on payload function, the attack may erase all project files from the file system, copy project files to some external locations. It can also spread to other servers which provide shared resources.

How this case can be recognized

- ▶ Indirectly. Check you anti-virus configuration and review all default settings for file exclusions.

Mitigation steps

- ▶ Review default anti-virus settings. Establish more restrictive rules for external data, email scans.
- ▶ Set up daily scans of important project directory and if malware is found force full scan of potentially affected resources, file servers, project workstations, local office and remote systems.

Case study #5: Vulnerable firmware in networked devices

Cyber-criminals may target not only the core company infrastructure or endpoints, but also the in-between devices, for which the security policy may not be specifically applied. In this example let's assume a typical internet provider, who offers services to end customers via DSL, Ethernet or other type of connection. When a user signs a contract with the provider, he usually receives a router, in order to connect several devices at the same time. The company supplies routers with pre-defined settings, making them easy to install and use.

The specific model of routers being used widely has a certain vulnerability. Router configuration can be accessed not only from the client side, but also from an external system. By using default and unchanged credentials, an attacker was able to modify the DNS records in a significant number of devices. This change resulted in slowing down the process of resolving IP addresses for domain names, which was noticed by users.

An attack of this kind can go unnoticed by the company, and pose a real threat for clients. An alternative DNS server may redirect users from popular online resources to infected of phishing web pages. The attacker can also collect user's credentials and even access the files on the client systems. Investigation, conducted by Kaspersky Lab's experts showed no sign of infection or other damage in this particular case. But in the middle of 2011 the company's anti-virus experts reported several cases, when Kaspersky Lab's security software detected a massive malware infection on otherwise legitimate resources, In this scenario the web resource in question (popular network statistics service or advertising network) as well as the client PC were not compromised, so it is evident that the users were being redirected from a legitimate resource to an infected one using modified DNS records or hostnames on the network level. Although it is nearly impossible to investigate these cases without having direct access to possibly affected network hardware, it is obvious that such incidents are extremely dangerous for businesses, because of the

high probability of infection or loss of sensitive data and the fact that the modification of network settings can be left unnoticed for a long time period.

How this case can be recognized

- ▶ Complaints from clients. The alternative DNS server, used by cyber-criminals, could not handle many requests, so the slowdown of Internet access was noticed. Unfortunately, after gaining access to this kind of devices, an attacker can use other techniques, which may be left unnoticed.

Mitigation steps

- ▶ Router settings have to be changed remotely to defaults, including DNS servers
- ▶ Access to routers has to be granted only for specific machines (user and/or company support)
- ▶ Default passwords have to be changed to prevent unauthorized access

Conclusion and security advice

Real-life examples in this white paper have demonstrated the ability to utilize IT security policy design mistakes by cyber-criminals. Even simple issues like missing security patches, wrong network file share security policy, mixed AV products environment, wrong access rights may put the entire company network at high risk. Kaspersky Lab had a vast experience in the field of IT security, and offers its corporate customers modern security solutions, which effectively protect businesses from all types of IT security threats as well as the consulting service to ensure the best experience and promptly provide help in complicated scenarios. Following is the advice from Kaspersky Lab's experts on how to tighten the corporate IT security system with simple, but effective steps.

- ▶ **Protect open files shares in the best possible way.** Always install the anti-virus solution on all public network systems. Follow the principle of least privilege. Do not grant write or full control permissions to everyone on remote file servers or on individual endpoints. Instead, try to minimize the number of users with elevated access privileges.
- ▶ Review your IT security policy and **define security updates schedule** to check for new updates at least daily. Use security solutions which allow to review the list of software installed, gather information about software vulnerabilities and available updates.
- ▶ **Control the use of Devices, Applications and employees' Web activity.** This is a key part of an IT security system, which enables to set simple rules on what external devices can be used, what software is allowed to run (or blacklisted) and effectively prohibits access to harmful websites. Although these three users' activities are controlled in some way in most of the companies, applying the rules and restrictions on a company-wide basis is necessary to effectively address security as well as productivity issues.
- ▶ Use **integrated security solution from one vendor.** Choose the one with high detection rates and ability for centralized control and management of IT security across the infrastructure.
- ▶ **Do not exclude non-executable files** from the anti-virus scanning settings.
- ▶ **Restrict usage of portable media** on critical infrastructure. Scan all files before backing them up.
- ▶ Regularly check with the manufacturer of specific devices (e.g. routers, WiFi access points, etc.) for **firmware updates and possible vulnerabilities.**
- ▶ Ensure that **default passwords are not used** on the devices and client systems.