RESELLER BRANDING

BEST PRACTICE GUIDE TO MAIL & WEB.

KASPERSKY lab

CONTENTS

LOCK DOWN YOUR SERVERS.

1. INTRODUCTION

Between 2011 and 2012, ninety-four per cent of all data breaches involved servers in some way.[1] It's hardly surprising – for criminals, the simplest route into your network is wherever the weakest point is. Too bad that's often your servers.

As the doorways to your company's network, the very functionality of mail and web servers makes them both highly vulnerable and desirable targets. Criminals use a variety of methods to seek out and exploit weak spots, targeting everything from software vulnerabilities to human error, gaining a foothold on your network from which they can launch more extensive attacks or steal vital business information.

Email's pivotal role in business communications has made it a particularly 'useful' attack vector. Every day, 89 billion business emails are sent and received worldwide.[2] Kaspersky Lab researchers have found that, as of September 2012, 72.5 per cent of all email traffic is spam; malicious files were found to account for 3.4 per cent of all emails.

From a web point of view, Google's bots detect 9500 malicious websites every day. In Q2 of 2012 alone, Kaspersky Lab detected and neutralised over one billion threats and a total of 89.5 million URLs serving malicious code. An estimated 80 per cent of attacks are aimed at web-based systems.[3]

Traditional anti-virus software on its own can't deal with today's blended, constantly evolving threats. Nor can IT professionals keep track of everything that's hitting their servers. Best practice calls for a comprehensive approach to server protection, using technology that can, among other things, filter out threats before they hit your network, block malicious content without impeding legitimate information and protect your servers without impacting on performance.

Here are some steps you can take – and technologies you can implement – that can help ensure your mail and web servers run at optimal security and performance levels.

1 Source reference: Verizon: Data Breach Investigation Report 2012
2 Source reference: Radicati – Email Statistics Report 2012-1016
3 Source reference: Top Cyber Security Risks Report, HP TippingPoint DVLabs, SANS Institute and Qualys Research Labs, September 2010

2. PROTECTING YOUR MAIL SERVER

Email's pivotal role in businesses of all sizes makes it the most vital and vulnerable link in the business chain. It's not just a communications tool – increased functionality has seen email used for document archiving, conferencing and calendaring, among other things. Research undertaken by the Enterprise Strategy Group indicates that up to 75 per cent of intellectual property is sitting in email data stores. No wonder email servers continue to be such an attractive target for criminals – both as entry point to the network and as source of commercially-sensitive information.

PROBLEM: As any IT administrator knows, email and groupware systems are under almost constant attack from spammers and criminal hackers. Even if they're not successful at stealing data or compromising your network, spammers can cripple bandwidth, while hacks such as relay theft can interfere with effective communications and cause network instability.

SOLUTION: Keep spam off your networks before it can cause trouble

- **Effective filtering:** The best way to deal with spam is to block it before it hits your networks, minimising the financial and resource costs associated with it. Intelligent, high-quality spam filtering technologies extend well beyond traditional, static keyword or block lists to include:

  – **Proactive monitoring:** Best practice calls for a solution you can train to know the difference between content you want to block and information you need. This is achieved by constant, automatic monitoring of messages to 'train' the spam engines to learn what can be rejected straight away and what can be quarantined or delivered.

  – **Reputation filtering:** Spammers change tactics all the time. Even a simple tweak to a keyword can confuse traditional spam filters. Reputation filtering categorises spam in such a way that it can block new attacks, even if the text of the message has been altered slightly. This not only helps keep you on a proactive footing, with near real-time protection, a high quality solution will allow you to block certain kinds of attack rapidly, without the need for analyst review. This saves you time and resources.

  – **Implement content filtering:** Monitor and filter email attachments according to your security policies. Block inappropriate email traffic (such as music files or videos) and potentially dangerous files (such as executables). Choose a content filtering solution that analyses files by content, blocking unwanted mail regardless of the declared file type or extension.

- **Black AND white:** DNS-based blacklists are one of the most effective configurations you can use to protect your mail server. These check message sender domains or IP addresses against global lists of known spammers – choosing a solution that gives you access to the maximum number of Domain Name System Block List (DNSBL) will enable you to greatly reduce the amount of spam getting through.

  Features allowing you to configure customised 'allow/deny' lists at both administrator and user levels will give you greater flexibility and granular control over messages. Developing your own, local blacklist can take time but is worth the effort, as it will help block spammers who target your servers specifically.

- **Head for the Cloud:** Constantly updated lists on a real-time database in the Cloud gives you an additional layer of protection, over and above your local lists and the lists on your solution's update servers. This gives you a rapid anti-spam response stance.

- **Identify targeted attacks:** Criminals are increasingly launching attacks specific to an individual business. Highly tailored spam geared towards specific themes or concerns in a given business is becoming a key vector for this kind of attack. Best practice calls for a solution capable of singling out attacks aimed specifically at your LAN – such spam messages are usually directed at a small number of key recipients. An anti-spam solution that works in concert with anti-virus can eliminate these attacks.

- **Enforce updates and adopt a zero hour approach:** One distinct feature of spam-related cybercrime is the "hit and run" nature of most attacks. Roughly half of any spam assault is delivered inside the first 10 minutes, meaning response times have to be just as fast. Kaspersky Lab's new solution integrates intelligent technology with a new Enforced Anti-Spam Update Service, offering rapid delivery of anti-spam database updates. This allows most spam to be quickly and efficiently blocked.

PROBLEM: Relay theft. Many spammers exploit vulnerabilities in groupware servers to steal the bandwidth they need to distribute massive volumes of spam. In other words, they use your servers to distribute their spam messages – passing all the costs and resource problems, not to mention angry customers, onto you. As a final insult, this often results in legitimate business communications being delayed while your overloaded server copes with pushing out the spam messages.

SOLUTION: All mail servers allow you to set restrictive mail relay parameters that specify precisely for whom your SMTP protocol should forward mail. Do it.

PROBLEM: Denial of Service (DoS) – Denial of service attacks can bring your mail (and web) servers and network infrastructure to a complete halt by flooding them with spam, sending more requests than it's able to handle.

SOLUTION: Limit the number of connections allowed to your SMTP server. Arriving at optimal numbers for acceptable loads can take time, and will depend on server specifications such as CPU and memory, but you should base parameters for connection limits around the total number of connections, number of simultaneous connections allowed and the maximum number of connections you can support.

3. ANTI-SPAM + EFFECTIVE ANTI-MALWARE = COMPREHENSIVE SERVER SECURITY

Spam isn't just a performance and resources issue – as Kaspersky Lab's senior spam analyst Maria Namestnikova points out, it's becoming more and more dangerous. "There is increasing use of malware that can infect a computer simply by opening an email. Spam also increasingly contains malicious links and fraudulent messages," says Namestnikova. "Malware in emails today is likely to be highly mutated, with no known signature or behavior pattern, meaning there's a very strong chance that an average web or spam filter won't pick them up until it's too late."

In July 2012, Kaspersky Lab noted a 50 per cent increase in the number of mails containing malicious files. Malware often opens up an entry point onto the network following a successful, well-targeted spam attack, such as a phishing email that persuades a user to click a seemingly legitimate link or open a seemingly legitimate file. The high profile RSA attack in 2011, for example, was executed via an infected Flash file embedded in an Excel spreadsheet entitled '2011 Recruitment Plan.' This mail was sent to only four, well targeted employees. The one person who opened the attachment retrieved the mail from their junk mail folder.

An anti-spam/anti-malware combination can give you the strength in depth you need to keep criminals off your server and network infrastructure. To complement your anti-spam stance, look out for features such as:

- **On-demand malware scanning:** Scan messages and attachments at file, folder and directory levels, as well as devices such as flash drives, DVD-ROMs and hard drives.

- **Real-time protection/zero-hour capabilities:** Frequent, automatic updates, real-time scanning and protection and access to a global, constantly updated global malware signature database will keep your anti-malware stance optimised.

- **Keep it quiet:** End users are quick to complain and will often seek to disable or bypass any processes they perceive to impact on system performance. Choose a solution that allows scans to run in the background, without interrupting users, allowing them to get on with their work.

4. PROTECTING WEB TOO

Web servers are highly targeted by criminals. As the 'shop window' for your business, many IT administrators take steps to protect the company website from attack – but leave the server hosting it (and all the applications and network connections associated with it) vulnerable.

Here are just a few tips for locking down your Web server:

- **Disable unnecessary services and application extensions:** You're pressed for time. You don't have the resources. So you install the operating system on its default settings and hope for the best… The problem with doing this is that many network services you don't need are left running, keeping ports open and using up system resources unnecessarily. Common culprits here include remote registry services, remote access and printer servers. Don't just switch them off, disable them – ensuring that they don't re-start the next time you have to re-boot the server.

- **Keep a tight grip on remote access:** This is difficult when workforces are increasingly mobile, but where possible, only ever log into your web server locally. If you have to do so remotely, use tunneling and encryption to at least ensure the connection is secure. Where possible, restrict remote access to a specific number of IP addresses and accounts.

- **Test in private:** You're testing out the new website or the application you're working on. You know it's full of vulnerabilities, so why have you left it sitting in a public directory, helpfully named 'test' or 'new application' for anyone to find and hack into? Test out new projects on a server that isn't network connected – and keep it well away from business-critical databases.

- **Keep permissions to a minimum:** Assign the bare minimum of privileges needed for any specific service to run – that way, even if a hacker or a malicious piece of code gets a toehold, they can't use that compromised service to carry out other tasks on your server.

- **Patch early, patch often:** Keep your system as secure as possible by ensuring you're running the latest version of the operating system, complete with all the latest security patches. Best practice here involves choosing a solution that will allow you to automate and enforce updates, so your server security is always up-to-the-minute.

- **Monitor everything:** Check logs regularly for suspicious activity. A centralised, single-pane-of-glass view of your network and web server will help you keep a close eye on what's going on.

5. SECURING THE WEB EXPERIENCE

Effective anti-malware software adds an additional layer of security to web gateways, ensuring secure web access for everyone in your organisation. Best practice requires automated removal of potentially malicious programs in HTTP(S), FTP, SMTP and POP3 traffic, but it's important that you also select a solution with load balancing capabilities, reducing the workload on your server or gateway and ensuring that everything runs smoothly.

Optimised, intelligent scanning takes a lot of strain off your servers and gateways – flexible solutions allow you to be flexible about what you scan, and when, increasing performance and reducing resources needed for effective scanning.

It's not just about scanning, however. Management tools and other features can drive an even more effective, secure web experience for both administrators and users:

- **Combined URL and content filtering:** As Google's bots have shown, many websites contain malicious code. It's not just compromised websites - on a daily basis, criminals launch and remove new, deliberately infected sites to catch unsuspecting users out. Users often don't even have to download anything – simply visiting the site is enough to infect them through unpatched vulnerabilities in their browser or other web applications.

  End users may not know the risks, but IT administrators do. You can't lock down the web, but a combination of URL and content filtering mean you can control not only how your end users interact with the web, but how the web interacts with your networks.

  URL filters recognise malicious sites and prevent users connecting with them. Content filters allow you to control what sort of content users can access, or limit the functionality of sites that may have been infected. You can do both without impacting on system performance and with completae end user transparency.

  Apply your roles-based security policies based around:

  – Individual
  – Group policy
  – Category
  – Web content

  Ensure that both your global URL and Content filtering databases and services are automatically updated from a constantly monitored, real-time database.

- **Monitoring and reporting:** Gain complete insight into what's happening on your network by running a solution that allows you to easily access information such as:
    - **Blocks per day:** Number of blocked requests over any selected period of time.
    - **Top categories by connection:** The most frequently addressed web filter categories by the number of requests.
    - **Top users by block:** The most frequently blocked users.
    - **Top users by connections:** Display your top users by request numbers.

Effective monitoring gives you insight into how your users interact with the web, facilitating more effective policy refinement. It also enables you to support productivity initiatives within the business – while ensuring strained resources aren't further burdened by bandwidth-hungry-yet-unproductive end user activity.

6. IN CONCLUSION

Organisations need intelligent security technologies to protect their data – and they also need intuitive and uncomplicated IT efficiency tools. Kaspersky Lab's 2,500 employees are driven to meet those needs for the 300 million plus systems they protect – and the 50,000 new systems a day that are added to their number.

Kaspersky Mail and Web Security solutions offer world class security for mail servers and internet gateways. Both are components of Kaspersky Endpoint Security for Business. Combining award-winning anti malware
and anti-spam, IT policy enforcement tools, centralised management and cloud-assisted protection, Kaspersky's business security products are the right choice for your organisation.

Talk to your security reseller about how Kaspersky can bring secure configuration to your servers, gateways and the networks they run on – and more!

RESELLER BRANDING

Reseller contact details

Tel: Email:

SEE IT. CONTROL IT. PROTECT IT.

With Kaspersky, now you can.

Kaspersky Lab ZAO, Moscow, Russia
www.kaspersky.com