GFI® white paper

Five security solutions for small and medium businesses and why you need them

Small and medium-sized businesses are increasingly becoming a target for hackers, scammers and social engineers. To protect the business's network, the IT administrator needs to assemble a broad range of security solutions to cover all aspects of IT security. In this white paper we highlight five technologies that will help protect the organization on every reasonably identifiable front.

GFI®

Contents

Introduction

Security continues to be the most critical IT consideration for all types of organizations, as well as one of the most important IT budget investments. With threats and risks being posed to business IT systems and data from a multitude of angles – including but not limited to malware, spam, application vulnerability exploits, data thefts, access control and inappropriate Internet use – IT professionals are challenged with assembling a solution to provide the best possible protection for systems, data and users, while at the same time ensuring a balance between cost, complexity, security and compliance.

The IT security market is an extensive one, with data from analyst firm Canalys revealing that the global enterprise security market was worth $22 billion in 2012 alone[1], while IDC predicts spending in the US is set to hit $5.6 billion a year by 2015[2], illustrating the breadth of solutions and the importance of IT security investment to businesses and the public sector.

Such is the broad nature of the IT security challenge in organizations today that no single product can offer a true "one size fits all" solution to security, or fit the entire security needs of a given organization, particularly for small to medium-size businesses (SMBs). Instead, IT professionals are charged with identifying and bringing together best-of-breed products in order to build an overall IT security solution that fits the unique needs of the organization and provides integrated, multi-layer security for all aspects of day-to-day business activity.

Evaluating the specific needs of the organization will require IT staff to audit both the devices and endpoints in use, and analyze how the organization uses IT, how it interacts with the wider internet and how it deals with external factors such as removable storage, remote workers, inbound communications and remote systems such as cloud services and customer or supplier portals.

The true cost of security threats

Due to their smaller size, SMBs can be forgiven for thinking they are not at risk and are not a target for external threats. What analysts such as Canalys argue is that security risks do not discriminate based on organization size, and a two-person company faces many of the same threats as one with 200 personnel. Furthermore, increasing data security legislation, designed to protect customers, suppliers and individuals about whom an organization might hold data, applies equally in most countries to all organizations regardless of size.

The cost of a data breach or theft in an organization is continuing to escalate, with the cumulative costs of response, recovery, lost reputation and fines mounting. Recent data from the Ponemon Institute shows that, in the US, the average cost of a cyber attack to business was $8.9[3]million , an increase of some 40 percent since Ponemon last surveyed. In the UK, the average cost to business of a cyber attack has hit £2.1 million[4]. The actual costs incurred by the businesses surveyed in the UK ranged from £400,000 to £7.7 million, while the same businesses experienced 41 successful security attacks a week – 1.1 per business every week.

The monetary cost of a single attack or data breach, coupled with the frequency with which businesses are targeted or fall victim to malware or other security threats, will often outweigh the overall investment cost of an IT security solution, providing it is strategically planned and deployed within the business.

Key questions to ask when examining the business for security pressure points:

- How many endpoints need protecting, monitoring and securing?
- What types of Internet/data connections does the business use?
- How many physical locations does the organization have?
- What types of data does the business generate and hold?
- What limitations are imposed on Internet access and websites accessed?
- What on-site IT support is available?
- What IT policy is in place and documented regarding IT security?

Answers to these questions will not only expose the key areas of weakness that need security focus, but also allow you to write or rewrite IT policy to support the technology being deployed. Without documenting IT policies in place to guide and educate users, the technology will not be as effective as it should be.

Top five security solutions for business

When approaching security for an SMB, there are five key technologies that should be considered as the building blocks for your overall solution: antivirus, patch management, email security, content filtering and network management.

Antivirus

Malware and associated malcode-based threats and attacks are undoubtedly the most prevalent and challenging security issue for companies to deal with. Ensuring that every client device and server is equipped with an up-to-date antivirus solution is an essential last-line-of-defense approach that all organizations need to undertake.

Antivirus solutions provide a variety of services to protect users, data and the core operating system from being compromised:

- Scanning existing files and storage devices for existing infections and compromised files
- Intercepting threats in memory as they try to execute
- Identifying known malware as it arrives on a PC by cross-checking against a regularly updated database
- Identifying and ring-fencing software and files exhibiting the known signs of malware using heuristic scanning technology

Antivirus software provides multi-faceted protection against malware entering and compromising a desktop PC or server. It acts as a barrier against identifiable malware trying to get on to a target machine via a variety of delivery mechanisms including removable storage, email, websites, direct downloads and compromised devices being synced.

It also acts as a container, trapping additional malware variants if they manage to get onto a target machine and attempt to execute. This is possible as some malware variants can prove difficult to detect when inert, so scanning during file copying or storage drive analysis won't always pick up everything. Capturing malware at the point of execution is possible by creating an in-memory sandbox, so that the malware can execute, but not reach any of the physical files or resources on the device in order to spread itself.

While trapped in memory, the antivirus software can either continue to quarantine the malware (and the physical file that carried it), or act as a cleaner to try and disinfect the contaminated file. The same applies during scanning of drives and file movements. Antivirus software provides the tools to clean files of their malware infection, or if that fails, can be used to safely eradicate the infected files to prevent further spread of the malware infection.

However, it is essential that the software and the virus definition files – the database of known malware and malware mannerisms – are kept up-to-date and that installations are monitored so that IT staff can ensure that overall network security is not being compromised by a weak endpoint. Therefore, an antivirus solution with a centralized management console, or one that can be monitored by an all-encompassing networking management tool, is essential.

Patch management

Effective patch management improves reliability and IT efficiency, as regularly updated software will be less exposed to vulnerability exploit and instability caused by bugs or attempted security hole exploitation.

The process of keeping a PC or server fully patched has been aided by the efforts of several key software vendors to build automated update checking into their applications, as well as the highly developed Microsoft Update service, which can download and, in many cases, install Microsoft operating system and application updates in the background without requiring user input or a system reboot.

Unfortunately, with the large variety of applications in everyday use on the average PC or server from a multitude of application vendors, users and IT professionals rely on running a variety of different update checkers or manually researching whether updates are available for a given piece of software. If left solely to the user, the installation of patches can be overlooked, leading to known vulnerabilities being left unaddressed and ripe for exploitation.

Dedicated patch management solutions, either in the form of a patch management server solution or patch management integrated at the desktop, can remove a substantial amount of patching burden from the end user and the IT department as a whole by consolidating the searching, downloading and deployment of patches into a single application that bridges multiple application vendors and centralizes the process to simplify management and monitoring of the patching process and the version levels of patches and software in use.

Being able to monitor which patches have been installed on which machines will also help in the rare occasions when a patch needs to be uninstalled and a machine rolled back to an earlier, pre-patched state. Occasionally, patches can introduce fresh problems to a system, such as instability or incompatibility that is only apparent after a patch is deployed. Centralized patch management allows for affected systems to be easily identified and rolled back with minimal disruption to the business and minimal time and personnel drain on IT.

Automating many of the administrative tasks associated with deploying software updates – while at the same time minimizing the amount of downtime associated with patch deployment, patch auditing and patch rollback – will benefit end user productivity as well as reduce the physical intervention the IT department will need to undertake to ensure that all computers in the business are regularly updated with the latest patches and service packs for applications and operating systems in use.

Email Security

Email by its very nature is one of the most challenging security touch points for any business and end user. As the primary form of business communication today, email is also the portal through which a variety of security threats can be express-delivered into the organization – from malware-infected email attachments to rogue links to compromised websites, phishing attacks and other scams. And it is a conduit for data to be leaked out of the organization, intentionally or otherwise.

Email security solutions allow organizations to address many of the risks and challenges posed by and posted to email services:

- Spam filtering to prevent unsolicited "junk" email such as unwanted promotional email, phishing attacks and other fake emails that purport to be from named organizations from reaching end users and end user machines
- Server-side antivirus scanning, placing the antivirus layer ahead of the end user in another effort to prevent malware from reaching end user systems by detecting it and impounding infected emails at the server, reducing the chances of infected attachments reaching and executing on a client PC
- Blocking scripting exploits in email body copy, whereby emails containing HTML and other code designed to exploit application vulnerabilities in email clients, web browsers and other applications can be blocked at the server level
- Email activity audit trailing to ensure that logs are kept of what emails are sent and received by whom, and what attachments are contained so that data leaks resulting from unauthorized sending of attachments and body copy can be traced or, indeed, disproved as needed

These security solutions should also be augmented with email archiving solutions to ensure that relevant but older email can be securely archived onto second-tier storage, but can still be easily and reliably retrieved in the event legacy email threads are needed for review or for compliance reasons.

Content Filtering

An important tool for all organizations regardless of size, content filtering solutions can be deployed either on the desktop or at the gateway, providing a mechanism to restrict which specific websites or types of website a user can access, what file types a user can download from the web and what types of content can be viewed while connected to the work network or while using work-supplied equipment on a public or home network.

Content filtering has two applications: productivity preservation and security enforcement.

The creation of site blacklists allow the organization to block access to web locations that are known to pose a security threat to the organization or user, such as being infected with malware, being a known destination used in phishing attacks or being known to contain illicit or illegal material such as pornography or incendiary material. This provides an important tool to prevent exposure to questionable and destructive code, ensuring that deeper security layers such as firewalls, antivirus and anti-spam solutions do not need to be called upon to defend the endpoint.

The creation of whitelists can allow organizations to limit web access on a given device, workgroup or active directory user class to pre-approved websites that are relevant to the work being undertaken, at the same time preventing the use of work computers, bandwidth and working hours for casual browsing of non-work websites and content such as social networking sites, video streaming services and chat forums.

Whitelists and blacklists are usually obtained from the application vendor as part of the regular in-application updates process and are based on regularly updated data from trusted sources such as malware and spam labs and specialists that trawl the Internet for troublesome sites and verified data about sites containing illegal or illicit data. These lists can then be augmented by the local IT team to add or remove sites as needed to enable smooth workflow and to block or allow access to legitimate sites and services as needed.

However, whitelists and blacklists represent just one part of the larger content filtering process. As with antivirus scanning, content filtering relies on not only pre-determined lists of known bad destinations, but also heuristic and predictive scanning technologies that can pre-empt exposure to inappropriate, illegal and otherwise unwanted web sites, web pages and material components within a web page.

Content filtering can also provide active scanning and analysis of web traffic and web destinations, looking for and highlighting the tell-tale signs of criminality, malware, pornography and other illicit or unwanted material. By analyzing keywords, body text, image types and file names, destination URLs, IP addresses and host information, as well as using other techniques including pre-caching web pages to see if they are using known vulnerability hacks such as cross-site scripting (injecting code from one site into the display page of another) or clickjacking.

Solutions also use reputation scoring and website classification as another means to determine how to curtail access. Cloud-based services analyze millions of web site and file requests in order to assign a score based on the likelihood of the target file or site being compromised. Scores are usually based on collective intelligence from multiple sources including:

- Vendor-specific networks of scanning nodes
- Intelligence from labs researchers
- Cross-vector intelligence from independent web, email, and network threat data sources

Combined with website classification, whereby sites are labelled as being a particular type (news, entertainment, retail, education, government, etc.), IT administrators can apply simple limits preventing initial access to particular blanket types of sites (unless included on the whitelist), or which do not meet the minimum reputation score. Or indeed a mixture of the two. Limits can also be imposed based on time of day, so stringent restrictions on retail or social networking sites could be relaxed during lunch hours or outside normal office hours, for example.

Limiting file type downloads has a multitude of applications, from security to prevent the opening of potentially infected files, but also to limit the use of work-based internet connections for the downloading of large, unnecessary files such as videos, audio files, games and other executables. File type limitations can be set to limit downloads to approved extensions and formats, such as Word, Excel, PowerPoint and PDF files for example, but even these would still have to pass antivirus screening and be from acceptable sources.

The same applies in reverse, allowing organizations to screen what files are uploaded in order to limit data leakage from the organization, as well as ensure that infected files don't originate from within the core network, leaving the business open to liability for spreading malware or other criminally malicious code.

Network Management

In addition to specific security solutions to tackle malware, exploits, email security and content filtering, robust network management and monitoring provides additional security safeguards and oversight of the entire network and the potential threats and weak points present on it.

Network monitoring solutions provide various tools and benefits including:

- Network auditing: Being able to build a complete and regularly updated map of what devices are connected to the network, what they are running, whether they are permitted devices and where they are, and to keep tabs on what they are doing
- Traffic monitoring: Observing network traffic for unusual surges, particularly busy endpoints and out-of-hours activity which can be signs of an infected endpoint, unauthorized use and data leakage, and vulnerability in network edge defenses such as firewalls and router configurations
- Vulnerability assessment: Scanning the network for weak points in the network topography, including analyzing the configuration of routers and switches as well as outward-facing devices such as servers, network printers and other devices that are accessible by remote and field workers to ensure these devices do not pose a security risk that could be exploited by external forces such as opportunistic hackers and denial-of-service (DoS) attacks.

Not only will automating these processes through software scanning cut the time taken to discover vulnerabilities and physically map the network, it will massively reduce the manpower needed to complete the task.

IT analyst firm Gartner estimates the average asset cost of a desk-side IT support visit to be between $35 and $250 per visit, with a phone call to a helpdesk representative costing between $10 and $37 per call. Rather than needing desk-side visits to investigate devices or wandering the building mapping computers and checking which ports they are attached to, the process can be triggered and overseen from a single console and a single window view, with the status of an entire desktop estate distilled into a single report, detailing exactly where to send expensive manpower in order to rectify any threats or issues.

Security in the cloud

In addition to deploying these solutions on conventional clients and on-premise servers, organizations are increasingly evaluating cloud-based solutions to solve security and compliance requirements while also minimizing the need for in-house expertise and dedicated hardware to manage and maintain these applications.

A variety of solutions, including anti-malware protection, anti-spam protection, and network and device management lend themselves particularly well to being delivered and operated from the cloud, allowing organizations to transfer the burden of server equipment, software installation, updates and maintenance off site and into the hands of professional service providers who can both handle the day-to-day service tasks while also passing on the economy-of-scale benefits associated with operating large-scale shared cloud infrastructure – benefits and cost savings not always accessible to all SMBs deploying and maintaining on-premise solutions.

Cloud-based security solutions work by installing a small local agent on the target machines that need to be managed or secured. This takes the form of a small software application that runs in the background and facilitates communication between the endpoint (whether it is a client or server) and the cloud back end.

Distribution can be simplified further by either pushing the agent onto machines as they connect to the network or distributing the agent via email. In both instances, the need for costly and time-consuming desk-side and server-side visits are reduced to almost zero.

Summary

Assembling the right set of security solutions for your organization requires that you first have a good level of understanding of the business and how IT security threats could compromise compliance, data integrity, productivity and competitiveness. For SMBs, ensuring that computers and other IT resources are safe, secure and free from the downtime associated with security threats is essential to ensure the business can function normally and cost-effectively, without tying up limited and often costly IT personnel to deal with the aftermath of preventable security threats and attacks.

Therefore, assembling a broad range of security solutions to cover all aspects of IT security is important and placing the five main technologies of antivirus, patch management, email security, network monitoring and content filtering at the core will help protect the organization on every reasonably identifiable front, ensuring that a duty of care is demonstrated to regulators and lawmakers, as well as to customers, suppliers and the organization at large.

Deploying security solutions to cover these five areas will ensure that disruption and downtime as a result of cyber attacks, malware infection, data loss and theft are minimized and, with it, the financial and reputational loss associated with such downtime. Keeping defenses strong and instances of failure to a minimum will also ensure that IT staff, often a limited personnel resource for smaller organizations, is not consumed fire-fighting breakdowns, infections and thefts and instead can concentrate on positive IT development and deployment that will ultimately benefit the organization's bottom line.

About GFI

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMB) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States, UK, Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold ISV Partner.

For more information about GFI and the range of solutions on offer for SMBs, visit www.gfi.com.

1. http://www.canalys.com/newsroom/enterprise-security-market-exceed-22-billion-2012
2. http://www.idc.com/getdoc.jsp?containerId=prUS23507912
3. http://www.networkworld.com/news/2012/100812-ponemon-cyberattacks-263113.html
4. http://www.computerweekly.com/news/2240164639/Cyber-crime-costs-UK-organisations-21m-a-year

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

33 North Garden Ave, Suite 1200, Clearwater, FL 33755, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit http://www.gfi.com/contactus

GFI 4357 jan13