GFI White Paper

# 10 steps to effective web security

## *Contents*

## Introduction

Achieving comprehensive Web Security is not a trivial task. The threat landscape of the Web is complex and ever evolving ... and implementing mechanisms to mitigate threats coming from the various risks is a difficult task. This is especially so for organizations with limited IT budgets, limited manpower, and other practical limitations. On the other hand, the Internet underground is a lucrative industry, and budgets are not spared on the other side. So achieving a comprehensive web security setup is a challenging feat by itself – besides all the other challenges that an IT administrator for a SMB has to face on a daily basis.

## Security at the perimeter

Rather than depending only on protection at the client-side especially with concerns to browsing security, a good safety net is handling web security at the edge/perimeter of the network. In this manner you are actually preventing anything malicious from arriving at the endpoint (the end users computer or other device) – problems are tackled at the edge of the network where any risk can be mitigated by keeping it segregated from the internal work.

Although your endpoints should have their own protection, your perimeter typically has much stronger defences than those available on the end point for various reasons:

- The capacity of the hardware in the perimeter is larger than that at the endpoint – thus affording multiple security mechanisms working in tandem
- It would be insanely expensive to deploy all security mechanisms at each point rather than at a single shared point in the perimeter
- Continuing on the previous point, keeping the perimeter well protected is cost-effective, thus a strong security approach can be taken which protects the entire network

The perimeter is effectively a "choke point" between the Internet and its wild nature and your more organized internal network. It serves a similar purpose of a physical, strong guarded gate – where the change in zone requires a checkpoint. Once again as with a physical site, you'd have a door possibly with a security guard and a receptionist – all offering different levels of security. It's expected that your network security exhibits a similar layered approach.

It is always better to stop a security threat once at the network perimeter than have to react and stop it at each endpoint. The cost of the single point prevention is always going to be much lower than cleaning up every affected endpoint.

Now that we've established that Web Security should be done first and foremost at the perimeter, we will highlight the methods of web security which are most effective.

## Antivirus protection

One of the first steps to achieving web security is scanning of user downloads. The biggest security threat posed by browsing users is when infected files are downloaded to the network.

***"1 out of every 14 programs downloaded is later confirmed to be malware" – Microsoft***

With such a large risk posed by malware, and with users typically being misinformed or unaware of the risks involved, anti-virus scanning is the first step towards a comprehensive web security implementation.

## Multiple antivirus engines

As with the principle of multiple layered approach to web security, this also applies to anti-virus scanning. Rather than scanning using a single antivirus engine, a multiple engine approach is ideal. There are several reasons for using multiple security engines.

- Multiple gates are better than one gate – since the engines are working together, the engines are complimenting each other. Anything not stopped by one engine is stopped by another one
- Don't put all your eggs in one basket – Although the bottom line of anti-virus vendors is similar, stopping malware, the actual parameters to do this vary significantly. Some are strong in certain areas and weak in other areas; some have quick response times to new threats, whilst others focus on covering all historical malware; some focus on speed whilst others focus on behavioural analysis. Obviously, in the web security business, you want to have all the strong points, but none of the weaknesses. With multiple anti-virus engines, you get multiple strong points, whilst the weak points of one anti-virus are covered by the other anti-virus engines.

## *Download prevention*

As discussed previously, the biggest threat posed is by user downloads of infected files. Certain file types are known to be potential security threats, whilst others are unlikely to contain threats. E.g. any kind of executable files pose a high risk, whilst other files such as ones containing text only are typically low risk. Most word processing packages now have script engines built-in that are used by malware authors to carry their payloads.

Although web browsing is typically a requirement or a need for many jobs, most users do not need to download and install files from the Internet. Allowing them access to download high risk files is an implicit security threat. Thus, as a proactive approach to web security, the IT administrator should actually implement policies which stop users from downloading these specific high risk file types.

It is important to make use of an engine which recognises real file types. One of the methods users try to circumvent this approach is to rename the extension of a file from something high risk, to something lower risk, and then renaming it when the file arrives at the endpoint. It is important that the security mechanism implemented isn't rendered useless by this approach – it is important that the real file type is actually analyzed – and stopped as necessary.

One understands that there will always be a need for certain users to have access to certain file types, so it is important that the different policies can be applied to different users and groups of users.

## *Content categorization*

The nature and the vastness of the Internet is such that you can find all types of content. You can find very helpful content such as educational information, news, hobby related and shopping information. However, there is a lot of content that you should steer clear of in the form of scams, fraudulent, phishing and malicious websites. Although the content varies widely, the categories of content on the other hand are not so numerous. You can easily list the types of websites on the Internet in less than a 100 "categories" of content. This is what a web categorization database is used for. It classifies websites based on their content.

Typically content categorization databases have a number of categories which are related to web security:

- Malware sites – sites that contain some kind of malicious content such as scripts or viruses
- Phishing and frauds – sites which try to defraud a user by accessing personal information
- Spyware and adware – sites which track users without their explicit consent
- Hacking – sites which provide information on illegal access to software or equipment
- Bot Nets – sites which are part of a bot net
- Confirmed spam sources

Using a web categorization database it is possible to block these types of websites and prevent access by your users. This ensures that users are prevented from visiting high risk websites.

## *Known malicious content protection*

"United we stand – divided we fall"

Whilst security vendors are in competition to sell their products, coming up with new and better ways of achieving protection and advancement in the web and total security arena, they are also doing many things together. Security vendors collaborate by sharing data on malware, so that when threats are discovered by one vendor, they can be rolled out to the other vendors as soon as possible. This has benefits for each vendor, and for the industry as a whole.

This leads to various sharing agreements – including lists of known malicious and bad websites. This is particularly important for sites which have been compromised and infected, rather than websites which are solely operated for malicious intent.

Websites which have been "hacked" usually provide malicious content for short periods of time – until they are cleaned. However, during the period in which they are infected – they pose a high risk to visitors.

A proactive approach to security would be to automatically block these sites which are currently known to be malicious – this ensures that users are blocked from access that website in the first place rather than reacting to the malicious content (i.e. hoping the antivirus solution can detect the strain). This proactive approach nulls any risk that the specific website might present.

## *Anti-phishing*

Phishing is another lucrative industry. The techniques have also evolved over time, and today the attacks use many complex mechanisms to glean the information from a victim. One of the latest is the use of what is called social engineering – where the perpetrator tries to earn the trust of the victim by using the names of organizations they trust, with emails seeming to come from legitimate or even internal sources and thus make the phishing scam look even more plausible.

The costs of a successful phishing attack can be very high – with either direct financial loss (bank or credit card details), or data leakage (confidential information) which would have very large indirect costs.

One of the requirements for a complete web security strategy is thus the implementation of an anti-phishing engine.

## *IM Blocking*

Instant Messaging is another service which can be used maliciously and thus a potential security risk. Besides being a potential severe productivity drain, the advanced features of Instant Messaging clients can lead to a number of risks, including:

- Malicious/infected files
- Phishing attacks
- Data/confidential information leaks
- SPIM (Instant Messaging SPAM)

Allowing the uncontrolled use of IM clients means introducing significant risk to the organization – and thus policies should be in place to ensure IM is only used if necessary and for reasons clearly outlined a policy for IM use.

## *Web Reputation*

Despite the implementation of the above mechanisms, most of the above features rely on detection of an existing threat. Web Reputation on the other hand is different – it is a prediction of the threat that a particular website might pose in the near future. The concept of reputation analyzes a number of website features to determine whether a specific site poses a security risk. An advanced machine learning engine also uses various metrics including:

- Location of website
- Behavior and Content of website
- Legitimacy
- Threat History

These metrics enable the engine to determine a score for each website. On the basis of this score, the website is placed into one of four security zones or bands:

- High risk (0 – 20) and suspicious (21 – 40)
- Moderate risk (41 – 60)
- Low risk (61 – 80) and
- Trustworthy (81 – 100)

This scoring system can be used to create policies on which websites users ca n have access too. For example, IT Administrators can access Moderate Risk websites, but normal users should only be allowed to visit low risk and trustworthy sites.

## *Education*

Although systems can help mitigate risks, no security system is 100% safe and the responsibility of web security remains with the end-user.

Educating users is paramount. The biggest risk to the organization or network is always the end user, so your strongest defense point is to educate them. Unless they understand that they need to be constantly wary when using the Internet, then they will always be a weak point. Users must have a basic understanding of the different types and methods of attack they could be exposed to whilst browsing. They need to learn to treat every site with suspicion by default, and be responsible for their actions rather than assuming it is solely the responsibility of the software and IT team to protect them. Tech-savvy users might also try to find ways to circumvent your web security measures, if they don't realize that their actions could cause irreparable damage to the network and the organization.

Ultimately this is probably the toughest challenge; however the highest level of web security would have been reached if that hurdle is overcome.

## *GFI WebMonitor*

GFI WebMonitor has been designed to cover as many facets of web security as possible without adding to an IT administrator's workload or impacting negatively on budgets. The Unified Protection Edition provides protection against all the above mentioned security risks. The primary goal is always to provide comprehensive protection at a low cost.

Security related features:

- Two antivirus engines, with a 3rd optional engine for scanning all downloads including downloads coming over HTTPS channels
- Download prevention policies using real file types
- WebGrade database covering 280 millions websites (and growing) in 77 categories including a number of security categories which can be implicitly blocked
- Automatic blocking of known bad websites – hundreds of thousands of sites known to be distributing malicious content are blocked
- Support for blocking popular IM clients
- WebGrade Web Reputation Index to allow blocking policies based on the reputation of a website

The best way to assess the web risk to your own organization is to try GFI WebMonitor.
Visit http://www.gfi.com/internet-monitoring-software to download and begin a 30-day free trial.

## *About GFI*

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMBs) 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 (North Carolina, California and Florida), UK (London and Dundee), 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 Certified Partner.

More information about GFI can be found at http://www.gfi.com.

GFI 2337 oct11


## 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

## ENGLAND AND IRELAND

Magna House, 18-32 London Road, Staines, 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