How bad are the bad guys?

The changing nature of Web security threats

By Jon Collins, November 2009

In a nutshell:

This paper considers how Web-based security threats are evolving, within the context of IT trends including mobile, home computing and other forms of remote access that could all potentially increase the attack surface of the organisation.

Key points:

- *Web-based threats are not going away, but they are changing based on an increasingly financially motivated community of online criminals.*
- *A number of mechanisms exist, each with their own benefits – the trick is to implement a layered approach that makes appropriate use of each one.*
- *Starting points for protection revolve around setting appropriate policies, raising awareness and implementing the right mix of protection.*

Introduction

The Internet has come a long way since its rudimentary beginnings as a government and academic network. At its heart it is fundamentally simple - allowing packets of information to be moved from one computer or device to another. But, even after the dot-com collapse when many said the Internet was 'done with', what we do with it continues to evolve.

Today we are seeing the Web broaden its reach to an ever-widening range of devices, and with increasing levels of interaction. Communications services such as WebEx and Skype take advantage of the greater bandwidth available in both home and mobile environments, and meanwhile social networking sites such as LinkedIn, Facebook and Twitter are rapidly growing in popularity.

While this is all very positive and welcome, due diligence requires that we turn our attention to the security risks that are posed by such changes in use and behaviour. It's quite trendy in security circles to talk about the biggest threats being internal, in terms of opportunistic breaches, loss of productivity through Web browsing and so on. Meanwhile, many organisations still see Web security as relating to viruses and malware infecting unprotected desktops. For many, it will be time to review these positions and act accordingly.

This paper considers some of the Web-related issues that might arise for individuals, and emerging or longer term threats that you may want to keep in mind when modernising or extending your security infrastructure. At the same time, security protections are evolving to meet such needs. Here we also consider what solutions are available and how to start deploying such new levels of protection.

This paper was compiled and written on an independent basis by Freeform Dynamics based on multiple studies during 2008-2009, within the framework of its community research programme and supported by Webroot. For more information on community research see http://www.freeformdynamics.com/services.asp.

The scale of the threat

What kinds of threats are lurking about in today's Web? As a starting point it is worth reminding ourselves that the bad guys never went away, but they too have continued to evolve. As they look for new ways to exploit holes in technology, they have become increasingly financially motivated, as illustrated by cases in the press of identity theft and credit card fraud. Organised crime has picked up where the 'hobbyist hacker', doing it for kicks, left off.

Perhaps the most significant trend is towards more intelligent, targeted attacks on both individuals and businesses. Big companies have lived with this for a while, being hit by those extorting money or causing damage for some political motivation. But with smaller organisations and their employees being more visible on the Internet than they have ever been, through their company Web presence, social media, and so on, there is both more risk of becoming a target, and more information available to attackers to work out how best to hit you.

So, what kinds of threats are we talking about? We can consider:

- **Malware, viruses and spyware.** Recent events such as the Conficker worm suggest nobody should be binning their desktop antivirus nor their content filtering tools just yet. Email viruses and malicious code continue to be a potential problem, but more of a risk today is that of spyware downloaded from the Web, which a user can inadvertently install at the same time as a 'freeware' program or a Web site plug-in. Spyware can be used to track the activities of the user (including logging key strokes, watching for potential credit card numbers and extracting other personal and corporate data), to act as a host for sending out Spam emails or denial of service attacks on Web sites, or indeed to serve as a relay point to infect other vulnerable computers.
- **Web page drive-by infections.** Building on the malware theme above, note that malicious content does not have to be downloaded or installed, but can be picked up even from innocuous and legitimate sites, if these have in some way been hacked. In the US, popular sports sites have been infected with malicious security code in the past, including major league baseball and hockey sites, and CNN Sports. Such code can then infect a desktop computer without any indication, just by visiting the site.
- **Social engineering and fraud**. In these attacks, a Web user is duped into doing something that will open them up to risks. Social networking has made this easier than ever, bringing many more people into potential conversations with Web-based strangers who may not be who they say they are. Recent examples include the use of truncated URLs (such as Tinyurl or Bit.ly) in combination with Twitter – the user is encouraged to click on what is claimed to be a video link, but which actually directs to a malicious site.
- **Misdirection and phishing.** This is where fake Web sites are set up to look just like the real thing, such that a user's identity details can be captured. A user may be directed via email or from another site. Even more clever are the ingenious 'man-in-the-middle' attacks which forward the user, via a corrupt Web site, to a real Web site such that username and password information can be captured as it passes through the corrupt Web site.
- **Denial of service and botnets.** A denial of service attack may be launched on a corporate or governmental Web site, either for extortion, or simply because of a difference in beliefs: the goal is simply to shut the site down, at least for a time. Attacks can be launched from the attacker's own computers, or by using so-called 'bots' or 'zombies' running on desktop computers that have been infected by certain spyware, as a 'Distributed Denial of Service' (DDOS) attack.
- **Confidentiality and data leakage.** Any information that is being transmitted over the Internet, must be considered at risk from being seen or in some way tampered with**.** This goes for corporate information as well as personal information: we know for example that Web mail accounts are a major conduit for confidential information leaving organisations. As we have already seen in the case of phishing, hackers can be quite innovative in obtaining personal details; adding social media into the mix, an additional challenge is that of information leakage which brings risks of its own. For example, there is now a site which 'follows' the Twitter feeds of top executives. Should the head of business development be broadcasting about potential M&A activity, or indeed where they are going for lunch? Another recent example involved the spouse of a UK security service head, sharing personal information on Facebook.

Just how serious are these risks? There are a number of Web sites which monitor such things, and while there is no need to panic, the general advice is to be vigilant. In the past, individuals and

organisations have set store in 'security by obscurity' – or otherwise phrased, "Why would anyone bother targeting me?"

The answer is twofold: first, the very mechanisms that have enabled the Web to grow so wide, have also given the bad guys broad scope when it comes to attacks (such as DDOS, for example) – everyone who is connected, is in some way vulnerable. Second, if there is money involved, then there is increasing likelihood of targeted attack. This is as true for corporations as for successful individuals. As technology continues to evolve – for example, in terms of virtualization, cloud computing, smart devices and so on – so do the innovative ways in which people can be exploited .

The challenge for many is the 'burglar alarm effect' – that is, when the majority of houses in the neighbourhood have installed burglar alarms, the few remaining become increasingly vulnerable, so it would be unwise to leave yourself unprotected when your peers are already taking steps.

What to look for in a security solution

So, where can you start when it comes to responding to the threats? Unfortunately, the answer is not as simple as 'buy a package'. There are a number of requirements on the information security architecture as a whole, which derive from the fact that security is more about managing a permeable membrane to the organisation, than trying to shore up the fortress walls.

It is important to implement protections that can evolve alongside any threats and changes in use, across all channels and wherever users might be connected. This may sound like a tall order, but what it implies is to provide an appropriate selection of protection mechanisms, deployed and managed in a co-ordinated manner.

The main options for Web security are not so much to do with what threats are addressed (the answer is 'all of the above, in some way'), but how they address them. There are three key places that you can apply protection: notably on the desktop, at the edge of the organisation (e.g. using a firewall or running a gateway appliance), or in the Internet itself. This last option is becoming more prevalent given the increasing interest in so-called 'software-as-a-service' (SaaS) based security applications.

Below we consider what are the required characteristics of security solutions, and the relative benefits and costs of each approach. Please note however that we do not see this as a one-or-the-other decision as each approach will offer a better fit to different needs.

Requirement	Desktop	Edge-based	Hosted security solutions
Threat protection	Protection at the desktop will always be a requirement given that malicious content can 'arrive' via USB sticks and removable media ; it also offers capability to remediate and remove existing threats.	This protection prevents bad things coming in, as well, as being a logical place to check for unauthorised information leaving the organisation.	Protection 'in the cloud' deals with threats before they even arrive at a company's site, as well as unauthorised information leaving.
Manageability and self-configuration	Desktops can be configured according to their specific needs, but each desktop requires configuring individually which puts pressure on management tools.	Offers flexibility in terms of setting a centralised policy and then applying it to all traffic entering and leaving the organisation. However flexibility comes at a cost of requiring more complex configuration.	Much of the management overhead of hosted security solutions (in terms of deployment, configuration, event management) is dealt with by the provider. However, self-configuration tools may not be as flexible as on-site capabilities
Management of updates	Updates to security tools can be onerous and may require manual intervention, which adds significant overhead across a large desktop estate.	Updates are limited to a smaller number of devices, and are therefore less of an overhead but still require manual intervention.	Updates to protect against new security threats are to all intents and purposes automatic, requiring minimal intervention.
Availability of skills in-house	Initial 'vanilla' configuration does not require in-depth technical skills, however delivering a consistent policy-based security configuration across the desktop estate does require knowledge and experience. See also edge-	Appliance-based models have the advantage of being pre-installed therefore requiring less experience to deploy. As with desktop however, skills to ensure that security configurations keep up with	Security skills requirements are reduced as the provider is responsible for most aspects. IT skills are also reduced. However, hosted security solutions require some knowledge to ensure they are architected in line with in-

Requirement	Desktop	Edge-based	Hosted security solutions
	based.	changes in policy and respond to new threats can be a burden.	house security capabilities (e.g. to avoid duplication).
Footprint of solution	Modern desktop security tools can run more efficiently than past versions, but the overall footprint has increased given additional capabilities that are incorporated.	Server-based edge protection may also add a load to existing servers. This can be offloaded onto a single device, in the shape of a pre-configured appliance, but internal power requirements may be the same.	Hosted security solutions have no internal footprint, apart from the minimal requirements of (generally Web-based) management software.
Legal compliance	Some on-site content security mechanisms (e.g. data leakage protection, anti-spam) may be viewed as illegal or contrary to worker agreements in certain geographies unless they are treated in the right way.	As with desktops, there may be legal issues with security filtering which can be dealt with by ensuring it is up to the user to define or accept reasonable policies, which can then be automated.	Hosting offers the possibility to filter inbound and outbound email and Web traffic to support company acceptable use policies. However some Web and email filtering services may not offer the granularity required to protect certain pieces of confidential information before it leaves the corporate boundary, for legal reasons.
Reach to remote locations and mobile workers	Desktops can be protected wherever they are, in principle. However remote computers are harder to keep updated than on-site computers. Home workers may be using their own facilities, which may require special consideration.	Remote workers lie outside the jurisdiction of 'edge' appliances, unless all Web traffic is routed (using VPN) via the corporate network which adds to network bandwidth requirements.	Remote workers can be given authenticated access to the Web via an internet-based proxy, providing the same level of protection whether the user is in the office, at home or on the road, and enabling centralised control of acceptable use and security policies for all users, regardless of location.

Note that all organisations are different, so it is a case of working out what is right for the organisation, in terms of what is already in place and what are the most significant risks and priorities. As is abundantly clear, there is no one answer and we would advise against putting all eggs in one basket, for example relying solely on desktop protection. Indeed, most security specialists advocate a layered, 'defence in depth' approach, with appropriate protection (to use industry parlance) 'in the cloud, at the edge and on the end-point'.

Not just technology!

The actual protections that you put in place will depend on a number of factors, including company size, business models and working practices, level of industry regulation, existing capabilities, procurement strategies and funding options. With so many things to think about, it can be difficult to decide where to start.

As we have seen in a number of research studies, the key to a successful security strategy is to balance technology with the needs of policy and awareness:

Policy

A first step is to understand what regulations apply to your specific organisation, which may have an influence on the approach you can or should adopt. Data protection law is generally accepted across Europe for example, but certain countries also have worker agreements that must also be adhered to.

Such requirements can be responded to with acceptable use policies (AUPs) to be agreed with the workforce. It's up to you to understand how they map onto your own business models and working practices. If you have a lot of people on the road or working from home for example, the approach you need to take will be different to if you are mostly office-based.

Policies need to be flexible enough to evolve as things change (for example to take into account use of social networking sites), and assume (this is an important point) prior agreement with senior management, without which they will quickly become useless. They also need to be acceptable to

the workforce otherwise they will prove difficult to enforce. Indeed, users may look for work-arounds which could pose an even bigger security risk to the organisation.

Awareness

One of the biggest security holes in any organisation is caused by "Users doing stupid things", or at least "Users not remembering what not to do". As such a great deal of time, effort and indeed money can be saved by ensuring that everyone is aware of the threats and AUPs, and what they can do personally to minimise the risks.

This further reinforces the need for genuine buy-in at an executive level. For example, there is little point in rolling out an information filtering mechanism across the organisation, if a board member then requests it is turned off so s/he can access a certain Web site on a lunch break.

As a final point, it is important to remember that while Web protection is an important element of IT security, it is only one facet of IT security as a whole, and business risk management in general. This is of particular importance when considering areas such as policy definition, employee risk management, staff training and external compliance.

Conclusion

While the future is impossible to predict, one thing we can say accurately is that the bad guys are not going to go away. They will continue to innovate and identify new forms of attack, and as economics becomes a stronger driver, things are only going to become more targeted. It is ironic in the extreme that the most vulnerable group is perhaps also the most likely to try to avoid protection – namely senior execs who don't see why such things apply to them.

While an organisation may not have been subject to attack, there is no room for complacency. This is not about panic, but being sensible – we can equate IT security with driving a car appropriately fitted with seat belts and air bags. We hope you will never need them, but we all feel more comfortable when they are in place.

Pragmatic implementation of the right technology in an appropriately layered approach, supported by the right policies and processes, is the way forward for organisations of all sizes. We hope the information and advice included here will help you, and those responsible for Web security to understand better the issues that exist, and to adopt appropriate approaches to solving them.

About Freeform Dynamics

Freeform Dynamics is a research and analysis firm. We track and report on the business impact of developments in the IT and communications sectors.

As part of this, we use an innovative research methodology to gather feedback directly from those involved in IT strategy, planning, procurement and implementation. Our output is therefore grounded in real-world practicality for use by mainstream business and IT professionals.

For further information or to subscribe to the Freeform Dynamics free research service, please visit www.freeformdynamics.com or contact us via info@freeformdynamics.com.