You need the good guys on your side

Introduction

Gone are the days when viruses simply corrupted your network, costing your organisation time and money to clean up the damage. Today's threats consist of 'under the radar' approaches in the form of multi-vector attacks, which operate across email and the internet and are designed to get past traditional security tools.

Email and web-based attacks like phishing and spyware are costing business and consumers loss in productivity and system downtime, financial losses, as well as and brand damage.

The need for creating certainty in all our exchange of electronic information is clear, whether this is across email, the internet, VoIP or instant messaging. Achieving it, without hampering the speed and continuity of business over the internet, requires some doing. Businesses today have a clear need for real time internet-level protection from known and unknown email and web-based threats.

In 2004, for the first time the proceeds of cybercrime – estimated at more than $105 billion - surpassed the underworld's profit from illegal drugs. Organised crime is finding a ready source of chinks in our complex, but often haphazard and reactive, electronic defences.

The indiscriminate mass mailing of infected code is fast being replaced by targeted attacks that use 'cyber tricks' to bait the hook. Online crime is evolving rapidly – and fast becoming more sophisticated and widespread, more determined and devious. And as attacks become more targeted, they're more effective.

Its most recent and most powerful manifestation is the multi-vector (or blended or hybrid) attack. Vectors are all the various connections a computer can make – and thus the way in which malicious code can infect your organisation. Vectors include email (SMTP), web browsing (HTTP), instant messaging, peer-to-peer networks, file sharing and Wi-Fi.

An example of a multi-vector attack involves an email entering an organisation and then enticing an unsuspecting user to activate an embedded link to a malicious website that infects the targeted network or computer. The attack jumps from one communication type to another, such as from email to web browsing.

Due to the level of stealth-like approach of these multi-vector attacks, it is far more difficult for traditional security software solutions to identify and remedy these approaches in real-time. The bottom line result is that your employees within your organisation could be at risk without you or them realising it, causing the potential for lost productivity, system downtime and/or financial loss.

Before the advent of multi-vector attacks, cyber crime came in three basic shapes: viruses, trojans or worms, which infect a computer and then propagate, choking bandwidth and disabling networks. Viruses and worms can also carry payloads – from irritating messages to highly destructive, costly commands, such as rolling back security measures and corrupting databases.

Unlike viruses, worms and trojans, which have a single mode of infection and usually require user activation, multi-vector, hybrid or blended threats spread in multiple ways, using email, instant messaging and peer-to-peer networks and exploiting web browser vulnerabilities. Multi-vector attacks are designed to evade single point security solutions and propagate as fast as possible. The huge rise in spam rates – estimated at between 60 and 77 per cent of all emails – combined with our increasing everyday use of the internet – makes us particularly vulnerable to the new multi-vector attacks.

Phishing is one of the most prevalent forms of a multi-vector attacks – and it is on the rise. Phishing, and its even more targeted variant, spearphishing (targeting specific individuals within an organisation such as the finance director or MD), is nothing more than a traditional confidence trick. But its criminal power is increased exponentially by the power of the internet through the use of spam.

Fake websites that are near-perfect replicas of a real business's website – except for a slightly incorrect web address and a missing or invalid digital certificate – are posted on the web. The criminals then unleash millions of spam emails, which also replicate the business's official communications. The spam directs recipients to the fake website and asks them to log in, providing confidential passwords and financial information. The replicas are so convincing that the Anti-Phishing Working Group estimates that around 20% of recipients click on the links, and 5% actually enter their confidential information.

The information can then be used to make illegal transactions, stealing from the spam recipient or from the business that has been used as bait. Or it can be on-sold to another criminal organisation.

Another example of a multi-vector attack at its most extreme centers around the installation of spyware, ranked as the second worst threat to enterprise network security in IDC's 2005 *Enterprise Security Survey*, and estimated by IDC to account for up to 30% of all helpdesk calls, with 67% of all computers having some form of spyware – in most cases, multiple programs.

Spyware is any software application that secretly gathers information about the computer user and sends it on to another user via the internet. Users can unknowingly download spyware from websites, through file attachments or through 'auto-install' applications. Traditional antivirus solutions cannot detect spyware, as they cannot 'catch' the self-propagating properties of spyware.

Spyware can simply cause annoyance and lost productivity through pop-up ads, consuming bandwidth and draining IT resources – or it can be put to devastating use by cyber criminals. In many cases, staff frustrated and annoyed by continual pop-ups generated by spyware, download pop-up blockers which themselves contain malware.

In some multi-vector attacks, spyware that secretly installs a keystroke monitor is distributed via spam. The keystroke monitor forwards everything that is typed on the keyboard to the criminals. Passwords, account details, credit card numbers, usernames and file data are all automatically collected, on a massive scale.

With an even greater potential to cost business dearly, some spyware can interrogate the system on which it's lodged, opening confidential files and uncovering network passwords –

placing at risk an entire corporate intellectual property, as well as lost productivity and the time and cost of disinfecting a network.

While there is anti-spam and cyber crime legislation, legal controls have limited effect as most spammers use off-shore email domains to transmit spam, and illegal techniques like address spoofing, trojans and the bot-net to conceal their identity.

The only real answer is for all businesses, large and small, to implement a cost-effective and multi-layered approach. The first essential step is the installation of real time protection at the internet server and desktop levels. Secondly, the introduction of a coherent and enforceable email and internet security policy to enforce practical measures to guard against damage to the information communication system. *The third and final step is critical, yet often neglected. All employees and users need to be educated about information security on an ongoing basis.* Security rules will not be kept without ongoing, active review and staff training. Staff also need to be reminded that their email and internet use can be monitored, so they can protect their own privacy.

Maintaining business continuity is critical, no matter what your business. A technological defence against known and unknown information security threats is the key element in any email and internet security policy.

Businesses can choose from a myriad of tools, which fall into three broad categories: appliance, software and Managed Service. Confusion exists in the marketplace about which of the three categories provides the most effective protection, and what the true total costs of ownership are.

Appliances

The appliance is a hardened server installed between email and internet server and network boundary, requiring set up and configuration to match the settings to the business's email and internet environment. As download volumes, bandwidth and security needs grow with a business, additional appliances need to be purchased to expand the network security capabilities.

Material must be downloaded onto the corporate server before an appliance can check it for infection. While the appliance is carrying out checks, bandwidth is compromised and systems are slowed.

With appliances, in-house information security expertise is essential to monitor malware trends, adjust appliance settings, configure updates, maintain and manage appliances, manage demands on storage and bandwidth and provide support to users. The total cost of ownership of an appliance solution invariably extends beyond the initial purchase price to include the cost of more than one dedicated, specialised IT specialist – which usually translates into a high opportunity cost for appliance solutions.

Software

Licensed security software is installed between the email and internet server and the network boundary, which often requires specific server hardware and software, adding to the infrastructure complexity. The effectiveness of a software solution is then totally reliant on it being kept up to date with the latest signatures to combat the escalating tide of emerging threats and unknown attacks. This presents significant ongoing total cost of ownership increases.

The public nature of software solutions can even work to undermine their effectiveness, as cyber criminals continually evolve their malware to work around security software.

Managed Service

While appliance and software solutions represent first generation information security solutions, their escalating and unpredictable costs and increasing scalability and performance problems have presented businesses with further challenges.

With the growing need for in-depth knowledge to keep up with increasingly devious and targeted multi-vector attacks, a Managed Service ensures a team of experienced information security specialists is always on hand to ensure seamless, real-time protection – at the lowest total cost of ownership.

The bottom line

It's not only business that benefits from the limitless potential of the internet – organized crime has now discovered its power, and turned enormous resources to undermining business's and consumers' efforts to protect electronic communications.

With unprotected computers estimated to survive 30 minutes on the internet, email and web security is of absolutely paramount importance. Moreover, the complexity, cunning and changing nature of the new multi-vector attacks – and their power to wreak financial havoc – means that specialist information security expertise needs to be on hand, up to date and staying one step ahead.

On the new battleground, business needs the good guys on their side.

www.encription.co.uk

01905 754440