

Cyber insecurity

As malware threats continue to get increasingly complex in nature, Web applications, are under siege.

BY ADITYA KELEKAR 

If ever the Web was considered as a highway for information, this year's security review shows that it has also proven itself as the freeway for insidious attacks. With successful exploitation of code vulnerabilities in popular programs and well-organized criminal groups launching more focused attacks, you find the user community is with its back to the wall.

Security vendors are coming up with new devices that specifically counter web threats, validate an endpoint before allowing entry in the network and bring out zero-day alert services in the wake of diminishing time period between the announcement of a vulnerability and appearance of an exploit code.

The Symantec Internet Security Threat Report for the period between July and December 2005 notes that unlike traditional attack activity that were motivated by curiosity and a desire to show off technical virtuosity, many current threats are motivated by profit. The threat landscape is getting dominated by emerging threats such as bot networks and customizable modular malicious code.

According to Niraj Kaushik, Country Manager, Trend Micro, India and SAARC, the total security market in India was estimated to be close to Rs 5,310 million in FY'06. The overall security products revenue touched Rs 4,260 million, registering a growth of over 41.5 percent over FY'05, and the security services market (consulting, managed security, and implementation) grew 45.8 percent to Rs 1,050 million.

One significant change in the mode of cyber crimes this year has been the shift from large multipurpose



AJIT PILLAI
Country Manager,
Watchguard

With the Internet growing in every sphere including e-Governance, the targets could be anyone

attacks on network perimeters to focused attacks on client targets. Kaushik says that new age hackers have evolved new strategies, launching quiet focused attacks. Instead of accessing a network and disabling multiple computers, hackers today seek to break into a network, stay there and collect organization's computing resources.

Ferdinand Gomes, Solution Specialist, Symantec opines that one of the most shocking revelations in India this year has been the discovery of a large amount of spyware that is found lying undiscovered on desktops. Gomes says this makes India both a target as well as source of attack. These along with phishing and spamming have been the most

dreaded security threats faced by Indian corporate.

While the Internet opens up Indian shores to 'war drivers' from across the world and vice-versa, the increasingly collaborative nature of business relying heavily on IP has meant that Indian companies are required to take security compliance seriously.

Surendra Singh, Head - South East Asia and India, Web-sense notes that most tier one BPO companies are required to comply with regulations like BS 7799, ISO 17799, Sarbanes-Oxley Act, HIPAA for healthcare and the UK's Data Protection Act.

The UTM Tide

The multidimensional nature of the attack as well as the increased threat incidence has meant that many more companies are looking at UTM with added interest. Harish Chib, VP-Marketing, Cyberoam, a UTM vendor, observes that while there has been a marked increase in

the variety of point products that have appeared to counter the threats, IT budgets have not increased in proportion and this is driving the integrated appliance market. "These appliances have proven to be cost-effective devices offering complete security," says Chib.

Vishak Raman, Country Manager, Fortinet, India observes that previously only larger companies bought network security solutions because greater dependence on the Internet made them especially vulnerable to hackers and crackers. However, now he notes that even smaller businesses cannot ignore network security because the current threats are not discriminating in their targets. Says Ajit Pillai, Country Manager, Watchguard, another UTM vendor, "With the Internet growing in every sphere including e-Governance, the targets could be anyone".

One of the casualties of UTM's growth has been point products. Vishak Raman notes that the firewall market is declining with the arrival of integrated security appliances.

It's not only the UTM vendors but even the bigger security players who have now learnt the trick of bundling a gamut of anti-x like anti-virus, then anti-spyware, anti-phishing and so on and packaging it as a single product.

Earlier this year, McAfee packaged a plethora of filtering features with its host-based intrusion prevention system (IPS) and claimed that the combination would require users to use at least 40 percent less resources. However, there are detractors to the claim that UTM can be the panacea for all ills. Kartik Shahani, Director Sales, India & SAARC, McAfee Inc notes that it is just not reasonable for a UTM vendor to manufacture the best-of-breed for all the constituent products. "If I am a CEO, I will buy best of breed products because one day's downtime on a critical asset can kill my business," says Shahani.

The individual defenders

While many users would go in for a UTM, there have been significant developments in the advancements in some of the point products that's meriting a closer look. One of them is Content Monitoring and Filtering (CMF) - a solution that monitors all outbound network traffic and generates alerts based on inspecting the data in network sessions.

In a recent press release, Gartner identified CMF tools

as a critical component in preventing data loss and information leaks. Says Rich Mogull, Research VP for Gartner "CMF tools are best at detecting and reducing information loss from accidents such as e-mailing the wrong file to the wrong person, or bad business process such as exchanging HR data over an unencrypted FTP connection."

The security issues in Instant Messaging (IM) are being turned a blind eye. "Most enterprises have barely begun to address the risk of virus, worm or malicious code attack through their employees' use of IM," says Surendra Singh.

Symantec's Gomes attests to the virulence of the malware coasting on the IM channel, noting that it can spread ten times or fifty times faster than a threat coming by an email channel.

Some sophisticated anti-spam appliances throttle the bandwidth for suspect traffic and opens up for genuine

ones. Gomes clarifies that these devices are not meant for everybody but for large companies who regard bandwidth as crucial.

The age of WAFs

A trend that is hardly surprising is the rising incidence of attacks on Web applications. Symantec Internet Security Threat Report for the period between July and December 2005 noted that 69 percent of the vulnerabilities disclosed were associated with Web applications. This represents a 15 percent increase over the first half of 2005 when they constituted 60% of all vulnerabilities.

The report notes that Web application vulnerabilities are particularly threatening because the applications are typically exposed to

the Internet through a Web server. Traditional security solutions such as intrusion detection systems and firewalls allow Web traffic onto a network by default, as such Web-based attacks are difficult to detect and prevent.

A new breed of protection devices called Web application firewalls (WAFs) is storming the market. "With this device, it's possible to 'vault' a critical piece of infrastructure - for instance, an ERP server in a manufacturing company," says McAfee's Shahani. With WAF, the IT administrator has options of scrutinizing the data flow through a set of processes.

NAC knocks at the door

Among the most revolutionary technologies launched this year was assessing the health of the endpoint device



KARTIK SHAHANI
Director Sales, India & SAARC,
McAfee Inc

PHOTOGRAPH BY SANDEEP PATIL

If I am a CEO, I will buy best of breed products because one day's downtime on a critical asset can kill my business

INFORMATION SECURITY

before allowing it access to the network.

The biggest advocate of this has been Cisco with its Network Access Control (NAC) - a set of technologies that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from emerging security threats such as viruses, worms, and spyware. Customers using NAC can allow network access only to compliant and trusted endpoint devices and can restrict the access of noncompliant devices.

This Cisco initiative that works in the realms of its proprietary systems hasn't met with cheers from all quarters. There is widespread recognition in the industry that an open-source, non-proprietary standard for network security is needed to meet the challenges of today's borderless networks.

This has resulted in Trusted Network Connect (TNC), an initiative of the Trusted Computing Group (TCG). The proposed standard is the result of the cooperative effort of 60 member companies with expertise in firewalls and anti-virus products; switches, routers and hubs; network security; systems management; and operating systems.

The existence of the two standards means a whole lot of additional work is taking place. Rajendra Dhavale, Consulting Director, CA notes that it is unfortunate that there have been two standards because the software, which is developed on the desktop will have to be compatible with both the standards.

How useful is the concept of NAC going to be? While Dhavale agrees that NAC's proactive approach of access restrictions is a helpful additional checkpoint, he notes that the patch management solution is anyway indispensable. Moreover, he notes that if the patch management process is adhered to, it is very unlikely that any desktop will be left vulnerable.

Dhavale is also wary of false positives denying legitimate access to the system.

The authentication scene

While the recent breaches of internal security in some of the premier BPOs have underscored the importance of strong authentication in the data-sensitive areas, companies from different industries are showing interest in having a tighter identity management.

Dhavale says that while many of the leading firms in

India have already deployed identity and access management suites over the last couple of years, they are now looking at a more structured way of doing things. For instance, if a user has ten applications, he is now looking at integrating all of them with a single access management suite.

As internal threats are rising in frequency and potency, linking identity to security is extremely critical to ensure effective security. Cyberoam's Chib says this involves taking strong authentication further and moving towards granular, individualized controls at the user level, in depth reporting based on user identity. "Such an end-to-end user identification, policy making, reporting and control based on user identity is the only solution against current threats," says Chib.



PHOTOGRAPH BY SANDEEP PATIL

The name of the game is no longer about detection, it's about the response

The security horizon

As the year moves on, one thing is sure: hackers will find ever-new ways to exploit security loopholes. Additionally, Web security for mobile phones will also assume importance in the future. Last year, malware writers began to target smartphones, particularly those running the Symbian and Windows Mobile operating systems. Websense's Singh feels that this year may see PDA and smartphone virus coders hone their skills, leading to a proliferation of sophisticated bugs.

An interesting outcome of the increased sophistication of attacks has been the efforts by many

leading software companies to consolidate their portfolio to offer services that address a broader range of security issues.

For instance, Trend Micro, a former best-of-breed vendor that specialized in antivirus now calls itself a threat management company in keeping with the changing nature of threats.

Trend Micro's Malav Patel, Global Product Manager, Enterprise Protection Strategy, Trend Micro says that today, a virus can be carrying spyware which can be a result of spam which can lead to more viruses. "The name of the game is no longer about detection, it's about the response - how you manage the response and it's about how you mitigate the threat," says Patel. It's precisely this response that will decide how Indian companies rise to the challenges that the complex world of information security poses to them. **NC**

aditya_kelekar@jasubhai.com