can create a separate zone altogether for visiting devices so that, even if they are infected, they do not affect other machines in the network.

Let's move towards threats that are keeping security heads of enterprises on their toes.

## Phishing

Protection against phishing and pharming attacks is very critical as most of these attacks target end users. Most of the gateway level solutions offer protection against phishing but majority of these solutions use blacklisting techniques to detect such attacks. Same technique is used for anti-spam solutions to detect phishing emails. However, this technique isn't always successful especially in case of targeted phishing attacks. Once a phishing email or URL manages to bypass an anti-phishing solution, it can even drop a malware into a user's machine which might even spread into other nodes of the network.

While buying a security solution, look for a solution which offers advanced phishing detecting techniques. Since now, phishing protection comes with Web browsers, security suites and anti-spam. So, at any point of time you will have multiple defenses against phishing attacks. For extra phishing protection, anti-phishing toolbars are freely available.

## Zero day attacks

Consider a scenario where a product is launched in the market that has some vulnerability. The period between patch releases to plug that vulnerability, and launch of product is known as 'Zero Day Period' and any attack carried out during that period is known as 'Zero Day Attack' (ZDA). To defend these attacks, there are number of zero day protection solutions available.

Most of the firewalls (Application level as well as gateway level) these days, provide protection against zero day attacks. Most commonly used techniques used to protect against Zero Day Attacks are behavior analysis, pattern matching, protocol anomaly detection. So while buying a UTM or firewall solution, ask vendorsfor solution that provide protection against ZDA. Many solution use signature based protection against ZDA, However in most cases, they only detect ZDA having signatures available. Such solutions are not recommended to protect against ZDA.

### LATEST THREAT

## Cache Poisioing in DNS Implementations

Recently researcher Dan Kaminsky found a critical bug in design of DNS(Domain Name System) protocol. Attackers can exploit this bug to control internet traffic and direct users to phishing websites and other harmful websites who could drop malicious software on users machines. An attacker basically poisons a DNs server cache and direct DNS client to a false website.

A test to check where your DNS server is vulnerable to this attack or not is available at researchers website at http://www.doxpara.com/. Several vendors have immediately released patches to protect against this attack.

## Some security solutions

### 1. Web application firewall

WAF is a new information security technology built to protect Web applications from malicious attacks. These firewalls are capable of preventing attacks that intrusion detection systems and firewalls cannot prevent. Another point worth mentioning is that these firewalls do not require any change in application's source code. These firewalls respond to all requests within OSI layer-7 for violation in programming security policy and usually sit between Web client and Web server and look for attack signature or abnormal behavior.

Web Application Firewalls are available as a appliance, third party plugins as well as software solutions. These firewalls are recommended for the companies who doing businesses online through web applications. These firewalls also provide protection against SQL injection attacks as well as botnets which are the major threats around these days. Such attacks can be easily combatted using Web application firewall at their initial level. ▷

## 2. Device based control: Cisco's Network Admission Control

This solution from Cisco is to enforce security policy compliance on users and devices in organizations.

Access to the enterprise network is controlled by giving access to only those users having proper credentials and dev ices that are compliant. These devices include printers, servers, IP phones, and wireless devices. Cisco's NAC helps in securing both managed and unmanaged assets of an organization. Proper management in turn lowers operational expenditure in long run and mitigates internal and external threats.

Cisco's NAC has following components: Cisco NAC Manager that is a Web based interface for managing NAC Server, where NAC Server is the actual device used to enforce security policies and is implemented at network level. Besides, there are three optional components. Cisco NAC Agent is a light weight read only agent on devices for inspection of their security status and for taking measures to make them security compliant. Non-PC device like printers, IP phones etc. are profiled using Cisco NAC Profiler that keeps track of their behavior.

Finally Cisco NAC Guest Server is used for automated provisioning, notification, reporting and management of guest devices.

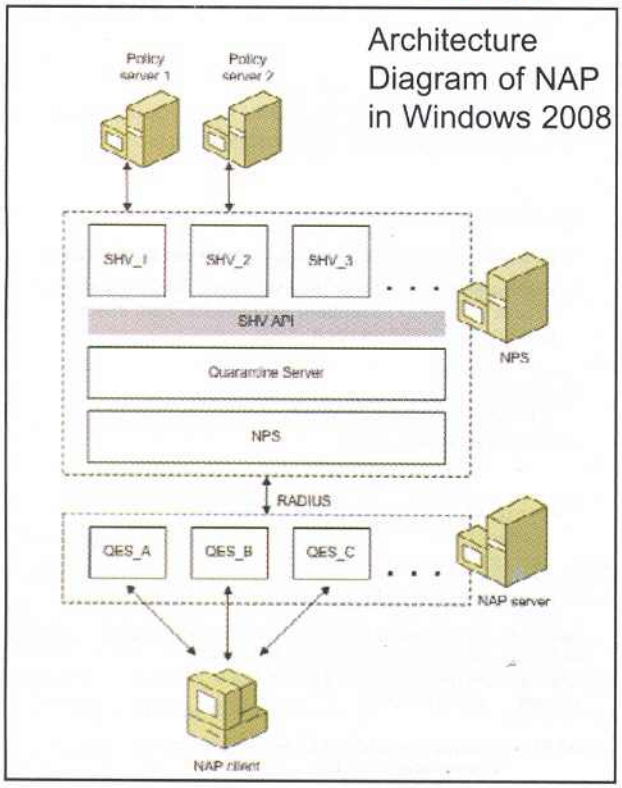
## 3. App based control: Microsoft's Network Access Protection

Approach taken by Microsoft for enforcing security compliance is application based. NAP like Cisco's NAC control access to network is based on devices' identities and compliances with security policies. NAP helps to define client's network access based on identity, group to which client belongs and degree of compliance.

If client is not compliant, NAP automatically tries to make client compliant plus it also includes application programming interface (API) for developers to create complete health state validation solutions.

Components of NAP are known as system health agents (SHA) and system health validators (SHV), these are used for validation and tracking of health state. Windows Vista, Windows XP service pack 3 and Windows server 2008 include NAP support for following type of network access: Internet Protocol security (IP-sec) protected traffic, IEEE 802.1X authenticated network connection, VPN connection, DHCP address configuration and Terminal Server Gateway connection.

These are known as NAP enforcement methods. Network policy server (NPS) in Windows Server 2008 acts as health policy server for these enforcement methods.




Source: Microsoft.com

## Physical security measures

One more important aspect of enterprise security is physical security. Physical security includes securing the work area by access control that can be achieved by access cards (RFID) or biometric measures and surveillance like IP surveillance .

If you want to know more about IP surveillance , refer to IP surveillance story in August issue of PCQuest. □

# 'F1' for Enterprise Security

**Security as a major concern, remains on priority list for organizations. We discuss here all that you need to know about such threats and solutions to plug the same**

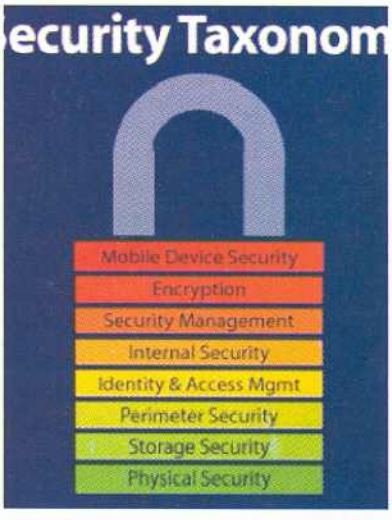
Swapnil Arora

Important data and information that lie at the heart of any enterprise needs to be secured to ensure smooth running of the business.

With connectivity reaching new heights, threats to nodes of information on network are increasing exponentially. With the advancement in enterprise security for networks, the number of 'successful penetrations' has also increased, making security a priority. Threat to information exists at every level be it your storage or network. Several solutions are available to do away with this threat, but striking the right balance of availability and security of information is a complex task.

For instance, blocking websites that contain words like 'sex' is not a good idea, as website hosting information related to medical field would also be blocked, which in turn may affect your pharmaceutical business. To simplify this complex task, there are domain specific consultants available with in-depth knowledge of security concerns and solutions to address concerns.

In this article, we will talk about various threats to information at different 'leak points', plus solutions available today to mitigate them. Finally, we will talk about security compliance.




Source: The451group.com

## Network security threats and solutions

One of the biggest sources of threats to enterprise security comes from Internet. Most of the spywares and viruses covertly reach machines via e-mail attachments or by 'piggybacking' on legitimate downloads. Once they get into a machine, it is very difficult to detect and eliminate. The policy of prevention is the best approach to tackle this threat.

Security at entry point to enterprise network should be properly implemented using gateway level security along with Web access control. Unified thread management or UTM's are fast becoming popular as single security device takes care of almost all the security related aspects of an organization. In a single UTM box, one can get security features like e-mail spam filtering, Internet traffic filtering, and anti-virus along with all the features of standard firewall.

These UTM's also include network management tools to further simplify network management. Having a single appliance for security also greatly reduce management issues associated with security. Customization of an UTM is quite simple with lot many free versions available today. One can build an effective UTM appliance by spending on hardware only. The only issue with these free versions is non availability of support, in case you run in to a trouble.

Another concern arises from ever increasing mobile device usage in organizations. If an infected notebook from outside is connected to Wi-Fi or to the local network, it compromises all preventive security measures. To overcome such a situation, you ▷

## BUYING TIPS

- Knowing security requirement before buying products is a must
- Get security packages from known vendors only
- While buying anti-virus or anti-spam software, check for available support
- Regularly update your security packages.An outdated package is as good as being non-existent