Policing the network

A robust network security policy is a vital part of any enterprise IT infrastructure. However, there are common pitfalls that should be avoided

Tlhe proliferation of intelligent mobile devices, web-based social media and now cloud computing in the enterprise mean securing the network is now more vital than ever.

The backbone of this protection is the corporate network security policy. In essence, this is a document or set of standards and workplace regulations that sets out some of the underlying architectures in an organisation's security environment.

"A Network security policies document contains a set of rules, privileges, regulations, processes, actions and procedures that describe the way users, machines and applications interact with each other and with the network infrastructure," explains Tarek Abbas, MENA systems engineering director at Juniper Networks, a US-based provider of network infrastructure equipment.

"[Network] security policies also outline all the network resources within a business and identify the required security level for those resources. Additionally, the network security policy defines security threats and actions taken for such threats," he adds.

Depending on the organisation, a network security policy may include stipulations that prevent users from plugging USB drives into the network, opening a PDF file, or accessing social media websites such as Facebook and YouTube.

Costin Raiu, director of global research and analysis at Moscow-based security software firm Kaspersky Lab, elaborates: "A network security policy is a set of rules and guidelines which define the basic architecture of the network, how different users can access various resources, how encryption is deployed and how routing of packets takes place between internal and external resources."

In drafting an enterprise network security policy, organisations should keep in mind the objectives that such a document aims to achieve. According to Mohamad Ismail, MEA security manager at Gemalto, a provider of digital security solutions, there should be two mains facets to these policies. "A good network security policy will focus on two elements: First of all establishing clear roles for who has the ability to do what within the network and secondly validating the identity of all persons accessing the network which means implementing strong authentication," he believes.

Responsibility for drafting and implementing a policy will usually fall with the enterprise's network or IT manager, who will take input from various information stakeholders from each department within the organisation. The final policy may then be signed off by a CEO or other similarly senior executive.

In terms of its coverage, a network security policy will generally account for a broad spectrum of IT and web usage across the entire enterprise. "These policies generally cover a wide variety of topics such as network management, traffic management, network operations, local security management and remote access," Ismail adds. "This could include internet use, social media, what can be accessed from where, [and] mobile device access."

However, network security policies can also be more granular than this, reckons Shanawhaz Sheikh, regional director at SonicWall, a company that makes enterprise network security products. An effective and well-implemented network security policy can allow selected individuals, such as management, to access websites and applications whose accessibility may be limited for the majority of employees.

"To give an example, let's say you would like to give full access to YouTube, but only to the executive management in the company," he explains. "So we define a policy where the executive management users get full bandwidth access to YouTube, while the remaining users get only 10% of the bandwidth and only between 2pm and 4pm, for instance. So this way, executive management [can] access YouTube without any restriction, and remaining users in the company have restricted bandwidth and time to access it."

MISTAKES AND REGRETS

There are a few common mistakes that should be avoided when drafting and implementing a corporate network security policy. One of the most obvious of these, says Mohamad Rizvi, manager of information security and advisory services at eHosting Datafort, a UAE-based managed services provider, is making it too rigid.

"Overprotection is one of the pitfalls for every organisation, as security is considered the most important element," he reckons. "However, these tighter controls might be a hurdle for conducting business. Users and customers get frustrated when they are not able to access what they are supposed to have access to. Therefore, security needs to be implemented in a way that business service doesn't get affected by having tighter security. There should be a balanced approach for security policy implementations."

Over the lifecycle of a network security policy, it is understandable

Technical controls are needed to reinforce network security policies, according to Gemalto's Mohammad Ismail

that it will naturally evolve as certain stipulations are removed, modified or upgraded. According to Rizvi, if this goes on without regulation over a long period of time, this can also create problems as network managers lose track and struggle to administrate the policy.

"The other pitfall is that over a period of time, there is a tendency of having too many policies and it becomes complex," he continues. "Due to business requirements, addition and deletion of policies may happen from time to time. Therefore, regular review of policies is good practice… these reviews need to be performed in a periodical manner."

There are other mistakes to be avoided when drafting and implementing a policy. For example, network managers should not rely on users adhering to controls by themselves, and appropriate technical mechanisms must be put in place beforehand. "The common pitfall is to have a policy that is not backed up by technical controls," elaborates Gemalto's Ismail.

"For example, in many information security policies the option is left to the end user to actually implement the best practices. A policy, for example, could mention 'passwords should be strong, long and contain special characters', but if such policy is not enforced technically, then the risks are always high that end users will most likely chose convenience over security."

It is perhaps no surprise then that experts recommend a significant amount of training is required to teach end users how to comply with the requirements of a policy. "This [training] should be a part of new employee on-boarding and provided on a regular basis to ensure all employees are aware of the policy," suggest Ismail. "Information security awareness programmes are available as part of HR training... and they are usually part of a new employee induction. Users should understand why some functions are not enabled within the network, why password sharing is not allowed, why a simple password provide a big risk and an obvious vulnerability, and on many other general information security topics that they will have to deal with on daily basis."

"There are no shortcuts to designing a security policy," **says Huawei's Steven Huang**

FURTHER COMPLICATIONS

The challenges associated with executing a network security policy can also differ across physical and virtual IT assets. With recent innovations such as virtualisation and cloud computing, traditional approaches to security policy may need to be rethought. "A key building block of existing policies is that boundaries are well defined and change comes slowly," claims Deepak Narian, MENA systems engineer manager at VMware, a large vendor of virtualisation software. "The model is simple: boundaries are defined, appliances are placed at the boundaries, and once placed they're likely to live a long productive life there."

"Virtualisation and cloud computing challenge both of these assumptions: boundaries are much more elastic, change is constant, new endpoints are appearing faster than ever before, [and] multi-tenancy is

Network security policies can be granular, explains SonicWall's Shanawhaz Sheikh

becoming a fact of life."

According to Narian, identity management and user access policies become significantly more complicated when applied across virtual infrastructure, and can no longer be based on physical characteristics such as location, IP or MAC addresses. Rather, security policies must have "tight integration with the virtualisation management infrastructure". "Existing policies either need to adapt, or risk becoming relics in the new order of the data centre," he adds.

Another recent trend that has complicated matters further still is spread of smartphones and other mobile devices in the enterprise. Ensuring that policies are equally robust across both wired and wireless networks is essential. "In case of wireless networks, the best approach is to only permit Internet access and then force the users to use a VPN (virtual private network) to access company resources," believes Costin Raiu, Kaspersky Lab. "Wireless networks have a higher chance of receiving unauthorised access, hence the higher need for better security."

Effectively designing, implementing and maintaining a robust, effective network security is ultimately dependent on the right blend of technology, strategy and user education, according to Steven Huang, head of enterprise solutions and marketing at Huawei, a China-based seller of network infrastructure. "A security policy must prevent inside and outside threats but it should also play a vital role in ensuring a seamless flow of business continuity. It's a trade-off between maintaining a level of security to protect the business' intellectual property without disrupting the flow of business for everybody," he reckons. "There are no shortcuts to designing a security policy. It's about finding a balance between one that is too restricting and one that is relaxed."

> "Businesses should take a balanced approach for security policy implementations," **claims eHosting Datafort's Mohamad Rizvi**

Security policy checklist

- Create a usage policy statement: This should be distributed among all of the company's end users. Ideally, it will contain guidelines for security best practice, users' responsibilities in terms of security, details of disciplinary procedures and tips on how to avoid falling victim to security breaches.

- Conduct a risk analysis: Complete an audit of the organisation's entire networking estate and possibly entry points for attackers. Each portion of the network and its accompanying infrastructure should be given its own risk level, as well as details of its types of users.

- Form a security taskforce: This team should consist of information stakeholders from across each department in the organisation. Essentially, this should act as the main source of design, implementation, and response for everything associated with the network security policy. The head of the taskforce should be someone with a technical security background, such as CIO or CSO.