

VNUNet – Fortify your IT defences to protect your assets

By Fran Howarth, Principal analyst, Quocirca Ltd

With the economic gloom worsening, the imperative for any organisation is to rein in the bottom line and cut costs.

Many organisations are responding by trimming their workforce. Not all will face problems, but a recent survey by the Department for Business Enterprise and Regulatory Reform found that the cause of the worst security incident suffered by 62 per cent of respondents was internal to their organisation, compared to 32 per cent in 2006.

The cause in these cases could have been inadvertent or a malicious act by a disgruntled employee, but such attacks can lead to sensitive information such as employee or customer lists being compromised.

Where a security breach leads to the leak of personally identifiable information, it is not only individuals who may be harmed. Corporate reputations can be damaged, and many of the regulations with which organisations must comply have real teeth and enforce severe penalties on those organisations that have failed adequately to protect sensitive data.

For example, the Payment Card Industry Data Security Standard requires organisations that handle credit card transactions to restrict access to the credit card data. As well as this, regulations regarding the notification of security breaches are becoming more widespread, and further legislation is expected soon from the European Union.

Information stored electronically is said to constitute as much as 90 per cent of the data produced by the average organisation today, and can be stored in any number of places from structured repositories such as databases and directories, to folders stored on individual devices.

In order to protect that information from being compromised, an organisation must put processes in place to ensure that it knows who is

accessing what data with which applications and when.

However, computer networks are becoming increasingly porous, and the perimeters harder to define, as the number of users and types of devices connected to the network continues to grow.

Mobile technologies are now commonly used to access the network remotely, and such devices often come with large information storage capabilities, making it easier for data to be misappropriated or just handled carelessly.

And many more devices are becoming IP-enabled, including VoIP phones, physical access control systems, building automation systems, cash registers and many industrial devices.

To prevent data leaks, organisations need to ensure that access to these disparate systems is controlled, especially where they are being opened up to access by external agencies or third-party business partners.

With this in mind, the onus is on organisations to develop an enterprise-wide risk management strategy, encompassing good standards of corporate governance and regulatory compliance, and with an emphasis on identity and access management, vulnerability control and intrusion prevention. So how can this be achieved?

One technology that is emerging from the shadows is network admission/access control (NAC). As part of an overall security strategy, NAC technologies can help organisations ensure that devices connecting to their network adhere with policies, such as access rights and having the latest virus protection turned on, so that all devices are in compliance with the required security posture.

Through device-level control, combined with identity checks, an organisation is in a better



position to regulate the resources to which each user has access via particular devices.

From its inception four to five years ago, NAC has proved a difficult child. Originally conceived as an infrastructure play, NAC technology was often costly and complex to deploy, in many cases requiring wholesale upgrades to an organisation's switching infrastructure.

Vendors offering this type of solution include Juniper Networks, Cisco, Microsoft and Still Secure, and their NAC technologies offer many advantages in terms of providing a single platform for end-point management, threat protection and vulnerability management.

However, as NAC technologies have matured, more choices have emerged in the form of software-based solutions, such as those from Intelliden and Sophos, and appliances from vendors such as Bradford Networks, Forescout, McAfee and Symantec.

Others, such as ConSentry, offer dedicated appliances and switch-based solutions. Software and appliance-based technologies can be deployed with less disruption than adapting the entire network infrastructure through a wholesale upgrade of all the switches in use, but they may not provide protection for the entire network unless, for example, multiple appliances are deployed.

This need not necessarily be a disadvantage, especially where business technology budgets are under pressure and organisations look to address specific points of pain.

For example, early NAC technologies were criticised for their inability to control guest and contractor access to networks, but there are now products on the market for solving particular points of pain like this, such as one of a range of new point solution appliances from Bradford Networks. The needs of specific vertical industries are also being catered for by vendors, including products aimed at the education market from Forescout and Bradford Networks.

Such vertically focused products allow organisations to concentrate on specific needs related to their industry, such as a large influx of

students at the start of a term with their own laptops that can potentially be mis-configured, contain non-compliant software or are riddled with viruses; or the high prevalence of shared kiosks in the healthcare industry, as well as the highly sensitive nature of medical records.

Deploying NAC technologies can bring many advantages in terms of improved security, automated compliance and reduced costs of managing user and device access to the network. As such, NAC is being touted as the next generation of intrusion prevention and vulnerability assessment technologies, combined with effective identity-driven access control.

However, NAC is no longer an all-or-nothing choice. The NAC sector has matured to offer more flexibility, enabling organisations to take a phased approach by focusing on the greatest problem areas.

That way, organisations can start by protecting their most critical end-points, ensuring that compromised devices do not get onto the network without breaking the bank. They can then expand the deployment over time by adding layers of fortification to their defences to ensure that all critical assets are protected.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, Dell, T-Mobile, Vodafone, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at
<http://www.quocirca.com>