Secure future

The year 2012 is dominated by three key trends – cloud, virtualisation and big data. These may be revolutionising the way people do business, but enterprises are starting to realise that current security systems are not sufficient to handle new threats. Ben Rossi reports.

With new security threats seemingly arriving by the day, and terms like 'hacktivism' and 'cyber warfare' becoming increasingly used in technology circles, the question CIOs really want answered is how do they protect their IT infrastructure?

A simple antivirus and firewall is no longer adequate – far from it. Organisations now need something more. That is where vulnerability assessment comes in. Industry experts now consider it an essential IT functionality and something that should be included as part of a company's GRC framework.

"We highly recommend the organisations across the region to adopt vulnerability assessments and vulnerability management solutions. In recent times we have witnessed cyber warfare being very active in the region, where big organisations have been victims of the process. Few immunity and security levels were tested to the edge," says Mir Ali, business development manager of the enterprise networking and security division at Emitac Enterprise Solutions.

Nima Saraf, team leader of technical application delivery for information security and cloud computing at FVC MEA adds: "Companies should consider vulnerability management because it is fast becoming an essential tool. Enterprises today generate an overwhelming amount of secure data but don't have the tools to turn this into actionable intelligence. Including vulnerability management as part of its GRC framework reduces security risk in the most effective manner."

Anas Ali Al Naqbi, senior security consultant at eHosting Datafort (eHDF)

Hostile environment

Anas Ali Al Naqbi, senior security consultant at eHosting Datafort, believes vulnerability management is one of the most important functions of IT security.

"In today's hostile environment, single-point solutions and a casual approach to vulnerability management are not enough. Security breaches result from known vulnerabilities and misconfigured devices. If new vulnerabilities are to be identified and addressed in a timely manner, then automated processes are required," he says.

Nicolai Solling, director of technical services at help AG ME, adds: "Everyone is talking about the threat landscape changing rapidly and having a vulnerability management solution as part of the IT security portfolio will surely make lot of sense. In addition, it holds a lot of value if one is thinking on the lines of risk of compliance. Having an in-house solution or engaging a consultant to do these tasks should be seriously considered."

Whilst it appears to be resoundingly agreed that vulnerability management is a vital part of a modern security IT infrastructure, that claim is often followed up with the warning that it should not be seen as a complete shield against all threats.

"Vulnerability management is not a 360 degree shield against all the possible threats but a tool which helps organisations to be more proactive. Vulnerability management products and solutions do two basic, but important, tasks. They help you discover the assets across your networks and they detect vulnerabilities. Vulnerability management is a comprehensive tool which allows organisations to identify, classify, remediate, and mitigate vulnerabilities," Ali says.

On-premise or managed?

After establishing the importance of vulnerability management and understanding its roll, the first step is deciding whether to opt for in-house scanning or select a software-as-a-service (SaaS) and managed services model.

Nicolai Solling, director of technical services at help AG ME

This decision ultimately depends on what the IT security directors, CIOs and CSOs are looking for, says Saraf.

"If the preference is over vulnerability data and integration of the vulnerability data with other systems, an on-premise solution is recommended. If the preference is to outsource security, a managed service may be an appropriate solution," he says.

"SaaS for security is still being developed as there are many questions about its reliability and security. The best approach to secure critical data and infrastructure is to reduce vulnerabilities rather than monitoring intrusions and attacks," he adds.

Solling says that whilst SaaS and managed services reduces work load by minimising management and operations efforts, it also means data is shared with the provider.

"Though the data is encrypted and not seen by the service provider, it always is a matter of trust. Depending on the SLAs that various providers have around these kind of services, enterprises might feel restricted when it comes to scalability of the deployment, frequency of the scans and reporting capabilities, which on the other hand will be more flexible when it is deployed in-house," he says.

He adds that he believes if organisations have the required resources and foresee frequent changes in the scope of the assessment, they should opt for an in-house scanning solution. However, Jacoby says he believes a hybrid solution is the best option and gives the customer full flexibility.

"Some companies have very sensitive information, and policies which say that all information should stay in-house. There are vulnerability scanning vendors which have both. They have SaaS solutions which can be integrated with an appliance that is managed in-house," Jacoby says.

Choosing solutions

When selecting a vulnerability management solution, there are several crucial components to consider.

"A strong authentication solution that secures the identity of users and applications that access non-public areas of an organisation›s network is the first step to ensuring data protection. The lack of adequate authentication mechanisms can result in critical vulnerabilities in organisation›s ability to protect sensitive information throughout its lifecycle," Pavie says.

"One of the areas where authentication vulnerabilities are most critical is online banking. In this electronic age, where banks are fighting off increasingly sophisticated cyber threats, it is vital that a bank customer's digital identity be protected at all times," he adds.

Mir Ali, business development manager of the enterprise networking and security division at Emitac Enterprise Solutions (EES)

Ali refers to the complex skills held by cyber criminals and their ability to expose hidden and high value vulnerabilities on a network, and that organisations should consider some key components before they commit to vulnerability management.

"When exposed, these vulnerabilities can be targeted for exploitation which may result in unauthorised entry into the network, expose confidential information, trigger theft of business secrets, or even paralyse business operations," Ali says.

"It should be able to define the policy, identify vulnerabilities, perform assessments and policy compliance, shield the environment, perform various assessments like attack, penetration and web application, and eliminate and track the root causes," he adds.

Organisations often want different components from a vulnerability management solution, Jacoby says, and many companies use it for different purposes.

David Jacoby, senior security researcher at Kaspersky Lab

"Some companies simply only use vulnerability scanning services and tools to become compliant, while others actually use it as a vulnerability management solution. But if you look at the components which are included in such a solution, and try list the most crucial components, I would say that they are asset and vulnerability management, a configurable score and scanning engine, and a report engine," Jacoby says.

Considerations

He adds that managers need to answer why they need a vulnerability management solution before looking for certain features, which he goes on to discuss.

> "Companies should consider vulnerability management because it is fast becoming an essential tool. Enterprises today generate an overwhelming amount of secure data but don't have the tools to turn this into actionable intelligence. Including vulnerability management as part of its GRC framework reduces security risk in the most effective manner."

"Does the solution have support for your language, or is it just supporting English servers? Remember that you can have sensitive data stored in files and directories with non-English names, and if their solution can't find it, it may miss a lot of vital information," Jacoby says.

"The vendor needs to have a good support team that can assist not just when a problem exists, but also assist in vulnerability management questions. Integrity of the service and product is also important. How is the data stored? Where is the data stored? Who has access to it? Is there some kind of ACL (access control list)?" he adds.

The process of selecting a vulnerability management product is far more complicated than asking who makes the best vulnerability assessment scanner, Ali says.

"Security managers should ensure that the vulnerability management product or