November 2013

Security in the network environment

Threats to network security are escalating dramatically. Technology advancements in social media, mobile devices, wifi and cloud services are increasing a company's vulnerability to attacks. Cyber risks and cyber threats are a major concern for large revenue generating organisations.

It is therefore crucial for organisations today to become more proactive and to invest in technologies that secure their networks and company data.

"To mitigate the risk of attacks, companies are now forced to improve security policies, that will ensure employees abide by rules that will protect the organisation's technology and information assets," says Laura Niehaus, Project Manager for EES, an ISO 9001:2008 certified company, which provides project management for the provision of information communication technology (ICT) solutions.

"These security policies are driven from the highest level in an organisation with security professionals who are frequently advising on security matters and compliance monitoring."

Even though organisations are moving in the right direction, there is still a need to analyse the current state of security in the network environment and identify areas of improvement. Health assessments focus on current threats and also help recognise potential new threats.

Access control

One of the ways in which network administrators control access to company data is by assigning user names and passwords. Standard security measures such as firewalls and proxy servers enforce access policies allowing users access to those services which they are entitled to.

"Although standard measures are effective in preventing unauthorised access, further systems are required to help detect and prevent harmful content," Niehaus explains.

"Intrusion detection systems, for example, should be used to detect malicious activity or intrusion attempts by outsiders and then log the activity for auditing purposes. Perimeter networking or demilitarized zones (DMZ) are also important in acting as a gateway to the public Internet and provides services to users outside of the local area network, such as email and web."

Key threats to network security

Data leakage, data loss prevention and data protection are major concerns. “Organisations usually cover data protection in contracts with third party vendors who have access to the company’s data,” Niehaus states. “Organisations should always implement enforceable contract clauses to make vendors responsible and accountable for information security that aligns to ISO standards.”

Niehaus continues: “Employee negligence or lack of awareness also poses a serious threat to confidential data. Organisations are developing and implementing policies to ensure a more responsible attitude by employees to confidential information.”

In large organisations it is important to increase the awareness of information security, integral to which is training, in order to improve policies. Employees need to be aware of their responsibilities and the correct use of company assets and data. Companies must employ staffwho have the right skills and competencies to support security policies and to make information security part of their performance assessments.

However, the trend of using personal smart devices for business purposes, allowing company information to leave the premises without authorisation, counters the principles of safeguarding sensitive data. Confidential data leaks can be the result of misplaced smart phones or tablets. This enables the introduction of malicious software into a company’s network, which could present damaging consequences.

Strategy going forward

There is a great need to align security strategy with business strategy. It is vital to be more proactive and explore new technologies that can help prepare for the future.

Processes need to be documented and communicated when opportunities for improvement arise, and budgets need to be made available to implement new security measures.

“Organisations need to shift their focus to security improvements, which will enable them to establish a framework for continuous improvement, proper governance, process, training and awareness.”

In conclusion, it is crucial to continually re-assess new technologies and threats, and always remain vigilant and listen to what is happening in the market.

-ends-

EES company profile:

Established in 2001, EES provides management, engineering and auditing services. As an ISO 9001:2008 certified company, it specialises in the integration of multiple system infrastructure including ICT, Data Centres, Audio Visual, Life Safety, Security and Building Automation Systems. With over 180 successful projects to date, EES operates predominantly in the Renewable Energy, Oil & Gas, Financial Services, Infrastructure, Utilities, Telecoms and Mining sectors.

EES is committed to proactively assisting clients reduce their carbon footprint and facilitate the development of a 'green' commercial environment. With offices in Johannesburg, Cape Town and Stellenbosch, it plays a key role in mission critical environments in Africa. Having successfully delivered on numerous international projects, EES' clients, partners and stakeholders benefit from the company's global knowledge and expertise.

Issued on behalf of EES
by ***Corporate Communication Services (CCS)***

For further information please contact:

Annabel Eaton
Corporate Communication Services (CCS)
tel: +27 (0) 21 702 3550 (CT, South Africa)
cell: 082 8984878
e-mail: eatona@netactive.co.za