Computer ResellerNews

http://crn.vnunet.com/Analysis/1136954

Network access is a question of privilege

Morgan Rees

Security used to be just about locking the door to hackers and throwing away the key, but no longer. A grey area has emerged which has more to do with the content you are granting access to than whether your user is a friend or foe. Controlling web access is fast becoming an important component of any successful security strategy. There are good margin opportunities for systems integrators that can help businesses develop and enforce corporate Internet policies.

Employees, partners, vendors and contractors all need access to an organisation's information, and not all of them are chained to the corporate desk. Many need remote admission. Networking environments are becoming more open and enterprise applications are being shifted to the web as businesses open their architecture.

With almost daily news of hackers penetrating large companies' systems, enterprises must recognise the connections between workflow, self-service management and

authorisation/authentication.

Authorisation and access control products help a business understand who is using its resources and who its customers are. Identification and authorisation procedures enable partners and suppliers to participate in electronic collaboration and help companies target customers more efficiently. Access control lists (ACLs) are the dominant method of securing the use of the Internet. Administrators can set common rules, such as blocking all employees from entry to particular sites or applications, and also enforce Internet policies for specific users or profile groups. They are easy to configure and quick to deploy. Some newer web traffic managers can support thousands of ACLs without affecting their server's performance.

Controlling access is not productive unless you have a way of recording what's happening. If you log the audit trails, they can prove beyond reasonable doubt that misconduct has occurred. Captured traffic is audited, logged and identified, and can be played back in court. Enterprises can also enforce electronic surveillance policies to protect intellectual property and reduce corporate liability.

Who you are and whether or not you are allowed specific access privileges is going to be one of the most important technology questions. The challenge will be to create secure inclusion.

Morgan Rees is a vice president of marketing