Netintelligence

OPINION SHEET

Embracing the Enemy at the Gateway

Utilising the power of the internet to overcome deperimeterisation

We operate in a mobile world.

As the demand for flexible working continues to rise (IDC predict that by 2007, 50 million Europeans will officially work from home) and technology continues to converge, the totally 'office anywhere' model will ultimately become the norm. There will be no constraints on how, when or where we chose to work. It is estimated that 82% of new corporate computer buys are notebooks, rather than desktops and that 74% of the notebooks are now wireless-enabled. Which is all very good news for the Dells and the T-Mobile's of this world, but not everyone is completely comfortable with this trend.

As IT administrators provide their mobile workers with their shiny new notebooks, and send them out into the utopian world of customer contact via the luxury of a Starbucks® sofa, very few of them are doing it securely. They are fast realising that the ground is shifting beneath their feet, and that a fundamental cultural change is required to counter their next challenge. The traditional and comforting world of the perimeter defence is no more. The single corporate network has now dissolved, and now extends through any number of worldwide hotels, airports, cafes and households.

In introducing flexible working, much thought has been generated around improving business processes and efficiency - but the solution for securing the mobile worker appears to have passed the decision makers by. The problem stems from a lack of money, time and knowledge, combined with that sinking feeling that end user behaviours can not be controlled away from base. The mobile worker presents businesses with a completely different beast to manage. And 'manage' is the key word here - mobile workers require management. Companies struggling to easily identify what the risks are for mobile users, and consequently do not have the process and policy models in place to counter them.

One current tendency in the attempt to address deperimeterisation, and mobile working, is to throw more technology at the problem. There is a belief that the problem can be addressed by extending the corporate network to meet the mobile worker, by pushing out more boxes, more firewalls, deploying more secure connections in a vain attempt to create an ever expanding safe environment, but this simply results in more cost, more complexity, more resource and ultimately results in little improvement. It's hard enough on a corporate network keeping machines fully patched and updated and ensuring that each end point remains compliant, but the issue is exacerbated when you have a mobile user.

It is blindingly obvious that many of the IT department's challenges regarding provisioning and supporting remote workers can be resolved by articulating, enforcing and reviewing a formal corporate mobile usage policy. The billion dollar question is how? There is an obvious but unconventional answer.

Every mobile worker in the world shares one thing in common, apart from the ability to complete their sales report from a deck chair, and that is that they have to connect to the internet to function. As many have discovered, it is often the simplest solutions that prove the most effective. The internet offers the perfect mechanism for the delivery and enforcement of security policy to the mobile end point, providing a ready made deployment, administration and reporting platform which can be controlled centrally but managed remotely. Organisations would not need to buy any additional infrastructure, they simply utilise existing architecture. A unified threat client installed on every end point has the capability to manage the activities of the user and protect at the same time. A constant communication process of data down and data back, whilst connected would deliver new policies, rules and anti virus/spyware signatures direct to the end point. The administrator would receive real time user activity and machine build reports - providing constant monitoring and a 'whole world' view regardless of the end user location, connectivity or time.

There is almost a delicious irony that, with many analysts agreeing that 'in the cloud' type services will ultimately become the defacto method for securing end points, organisations may have their security policies delivered and enforced by the one thing that they have spent the best part of two decades protecting themselves against ….the internet.

For further details:
Netintelligence.
www.netintelligence.com
or email:
info@netintelligence.com.
Tel: 44 (0) 870 050 0121