MOBILE AND REMOTE WORKING: IS IT SECURE?

Submitted by: Annabelle Brown
Wednesday, 12 March 2008

By Ian Kilpatrick, chairman of Wick Hill Group, specialists in secure infrastructure solutions

12th March 08

580 words

Summary of feature

* Unstoppable move towards remote and mobile working

* Mobile working is not adequately secured.

* Organisations are concerned about security for mobile and remote workers and how to enforce company security policies outside the gateway.

* Companies want to protect against data leakage and data loss from such problems as stolen laptops.

* There is no one solution to securing remote working.

* The range of solutions includes strong authentication, end point security, remote unified threat management (UTM) systems, low-cost encryption and VPNs.

The move towards remote and mobile working seems to be an unstoppable trend. Research by ZDNet.co.uk and market intelligence company Rhetorik found that the penetration of mobile workers across the UK workforce is significant. Nearly a quarter of all organisations considered more than half their staff to be mobile workers.

Mobility, the research found, is an upward trend with nearly two-thirds of the research sample reporting an increasing proportion of mobile workers.

Mobility is clearly where users and companies want to go and it undoubtedly has major benefits. It brings freedom and reduced costs, but you still need to secure it. Security deployment, as is often the case, has lagged behind the rapid growth of technology and a significant number of staff are now working outside the protection of the company network gateway.

Organisations worry that mobile working will get beyond their control and cause problems both inside and outside the gateway, resulting in data loss and introducing malware.

They are increasingly keen to ensure that the same policies and security they deploy at their corporate gateway are also provided for their mobile users. This is for compliance and legal requirements, as well as for security reasons. Another issue around mobile use, very topical at the moment, is that of organisations wanting to protect against data leakage and data loss, from such problems as stolen or

mislaid laptops.

There is no one hard and fast solution to securing mobile and remote workers. Strong two-factor authentication, which ensures the identity of the mobile user connecting to the network or using the laptop/mobile device, is a basic requirement. Static passwords are woefully inadequate, with huge identity theft risks (particularly for wireless). Low-cost strong authentication solutions are available from vendors such as CRYPTOCard and VASCO.

Increased remote working implies increased security at the end points and there is a wide range of solutions available including remote firewalls and specific end point solutions, which can be administered centrally. Such solutions can extend network protection strategies to mobile and remote users. They can also ensure that firewall, anti-virus and security patches are used by remote and mobile users when they should be.

Check Point provides 'End Security', an end point security solution which combines a firewall, network access control, program control, anti-virus, anti-spyware, data security and remote access. It allows security policies at end points to be viewed and modified from a single management console.

Branch offices can install low-cost remote unified threat management systems (UTMs) which incorporate VPNs and these can be centrally administered, typically by the head office, providing the same levels of gateway protection as there is at the centre. SSL VPNs can provide security of data in transit for mobile users connecting into head office or between branches.

Solutions such as WatchGuard's Firebox SOHO Edge (available in wired and wireless versions) and Check Point's UTM-1 Appliance are UTMs suitable for remote/branch offices which combine a firewall, VPN, zero day protection, anti-virus, anti-spyware, anti-spam, intrusion prevention and URL filtering.

Low cost encryption can protect remote laptop users and safeguard against data loss. In the past, poor performance and high costs prevented the use of encryption software, but today's high performance and low cost solutions make it impossible to justify not encrypting laptops. Low cost solutions from encryption specialists such as Utimaco can protect network data, laptops and removable media.

Finally, wireless is high risk and all mobile wireless traffic should be over VPNs and be encrypted, with the use of strong authentication.

ENDS

Bio – Ian Kilpatrick

Ian Kilpatrick is chairman of value added distributor Wick Hill Group plc, specialists in secure infrastructure solutions. Kilpatrick has been involved with the Group for more than 30 years. Wick Hill is an international organisation supplying most of the Time Top 1000 companies through a network of accredited resellers.

Kilpatrick has an in-depth experience of computing with a strong vision of the future in IT. He looks at

computing from a business point-of-view and his approach reflects his philosophy that business benefits and ease-of-use are key factors in IT. He has had numerous articles published in the UK and overseas press, as well as being a regular speaker at IT exhibitions.

About Wick Hill

Established in 1976, VAD (value added distributor) Wick Hill specialises in secure infrastructure solutions. The company's portfolio covers security, performance, access, services and management. Wick Hill sources and delivers best-of-breed, easy-to-use solutions through its channel partners, providing customer support, implementation, technical services and authorised training courses.

For further press information, please contact Annabelle Brown on 0191 252 8548, email abpublicrelations@btinternet.com. For reader queries, please contact Wick Hill on 01483 227600, web www.wickhill.com.

response**source**