SSE® Network Services

Mobile Device Security for Small Businesses

By Elizabeth Elliott Niedringhaus
President and CEO of SSE

From smart phones to netbooks, there are an increasing number of sophisticated tools that small businesses can use to go mobile. Yet, according to analysts and security firms, many companies are just beginning to wake up to the challenges of implementing device security policies, and awareness is still below where it needs to be. Without a doubt, mobile devices offer greater flexibility and better productivity by allowing employees to work outside the confines of brick-and-mortar operations. However, along with greater mobility comes greater responsibility, namely in the form of managing security. The good news is that device management solutions don't have to be complicated or expensive.

One of the top concerns is the inadvertent sharing of data. It's very likely that someone might mistakenly send out sensitive data from their phone. Another key issue is what to do when a smartphone is lost or stolen--and how to turn that phone into an un-useful brick. Even if a company decides it is not going to pay for their employees' devices, it is still responsible for the data on them. Having the ability to remotely wipe a phone should be a core requirement of any company's device management and security policies. However, according to Winthrop from Strategy Analytics, only 50 percent of U.S. organizations have "remote kill pills" in smartphones to shut them down, and less than 50 percent have the ability to remotely wipe the phone's data card.

Mobile devices are just as, if not more, susceptible to malware as PCs and laptops are. Users download applications and open e-mail attachments every day on their mobile devices, resulting in many infected networks. Companies need to deploy appropriate antivirus and anti-spam solutions to protect against malware. Each device must be equipped with a VPN client to encrypt mobile communications traffic and a firewall to prevent targeted attacks on in-transit data. Smart hackers will always go for the easiest target, and new technology is often fertile hunting ground. As with any other security strategy, awareness and education are crucial. Users have to understand the risks their mobile devices pose and the consequences of a security breach.

Another safeguard is to keep devices up to date. Make sure all handhelds, PDAs and portable computers have the current software updates and security patches. It's also a good idea to limit access to sensitive data as well. Not every sales member needs access to company financial data. Using a firewall can help limit mobile users' access to sensitive information. In this way, a phone left in a cab won't become a liability.

Ultimately, the best way to ensure that mobile devices are secure is to establish a formal mobile security policy. Document all obligatory actions and processes and disseminate the information among your employees. You should also communicate urgent security updates or notices via e-mail.

SSE can help secure your mobile network. We can give you a peace of mind to mobility, with strong knowledge of the threat environment and an equally strong arsenal of security tools. Contact SSE today!