Ubiquitous Internet Dial Tone

by Robert L. Gezelter, CDP

My friend and colleague Robert L. Gezelter, CDP, has contributed an interesting article on the security and accessibility implications of pervasive workplace Internet access. The following is his text with minor editorial changes.

--MK

***

Over the last decade, laptop computers and network technology have become almost universal in workplaces. Many or most of the employees toting laptops are not field personnel; indeed, most of them rarely leave their office buildings. So why are companies spending extra money to pay for laptops?

In a recent speech, Andy Bryant, Intel’s CFO, stated that issuing employees laptops instead of desktops was a reasoned business decision based upon costs of business operations, not on employee convenience. His staff found that meetings were pausing, or failing to reach answers, because of the absence of information normally available on employees’ personal computers. Bringing laptop computers to the meetings closed the information gap.

The next logical step has been to access the corporate network using wired (10/100BaseT) or wireless (WiFi) connections, bringing additional information into the decision making process. However, this scenario raises major security issues.

Protected facilities with wired connections for each machine, where everybody has the same access to the corporate network are the simplest, and admittedly, the least interesting example. More illuminating is the common situation where the network is wireless, the attendees are a diverse group, and the access to the corporate network is different for different classes of attendees. Some meeting attendees will be outsiders with no access to their hosts’ intranet, yet requiring access to their home company intranets. Sometimes outsiders may be friendly; e.g., members of the project team from other participating companies. In other situations, the outsiders may be less than friendly; e.g., customer technical and managerial representatives, government regulators, or inspectors.

We need to provide secure access to appropriate information for both employees and visitors. We can do so by implementing a hierarchical security system. The solution is to treat network access as a digital dial tone available to residents and visitors but with security restrictions enforced after the users have connected to the first layer of the network services.

WiFi security has a place in the security spectrum, but that place is as a coarse screen to keep random interlopers at arms length. As for wall jacks linking to wired LANs, the most cost effective solutions use VPN technologies to provide secure access to authorized personnel and the ability to deal with the full nuances of the security environment within the corporate intranet. Everyone else just gets access to the external Internet.
MK adds: even there, visitors’ use of corporate Internet access should still be controlled by firewalls using egress filtering to ensure that visitors are not making the host facility liable for damages or criminal prosecution by engaging in acts such as denial of service attacks or downloads of child pornography.]

***

Robert Gezelter, CDP, Software Consultant, guest lecturer and technical facilitator has more than 25 years of international consulting experience in private and public sectors. Mr. Gezelter is a frequent speaker at technical conferences worldwide such as HPETS (formerly DECUS) and a member of the IEEE Computer Society’s Distinguished Visitor Program. In March, he will be speaking more elaborately on these issues at two Central Florida IEEE Computer Society chapter meetings (Tampa on March 24, Orlando on March 25).


Bob Gezelter can be reached via email at <mailto:gezelter@rlgsc.com>. His Web site is <http://www.rlgsc.com>.

***


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2004 Robert L. Gezelter. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.