

# Protect the road warrior

... and deter the black hats

**Security has become paramount on mobile devices as more employees work away from the office. Ron Condon investigates.**

Just when you thought you could relax, an ever-evolving challenge is facing information security professionals. A growing army of mobile workers is demanding to have the same level of access to systems and data as those back at the office. Your mission, should you choose to accept it, is to make sure they get it securely.

The dangers are obvious. Laptops holding sensitive data can get lost, damaged or stolen. Data sent from the local café's wireless hotspot might be intercepted. Unwanted intruders may pose as employees and try to penetrate the corporate network.



The advantages for business are equally clear. "Our customers rave about the increased productivity," says Carey Balzer, president and chief executive of TManage, a provider of managed security services. Through an alliance with the worldwide iPass

system, which offers 20,000 points-of-presence for mobile workers to dial into, TManage delivers a combination of managed firewall, anti-virus and VPN facilities for companies across the U.S. and Canada.

"If I'm waiting in airport security, I can get a [wireless] 11Mbit/sec connection and do a 20Mb update on my Lotus Notes. This means I can have two or three hours of productive work on the plane. Within two minutes of getting off the plane, I can send off my work. It allows business to flow on a real time basis," says Balzer.

He adds that by installing broadband in employees' homes, many companies are improving both the productivity and the satisfaction of their staff. "Some companies report a 15-17 percent reduction in staff churn," he says. "Employees can achieve a better balance between their personal and professional lives, and they can also check mail and do work from home."

Salespeople and field service engineers have long worked remotely, sending information back to head office using a variety of remote access schemes. But these, and many new categories of workers, are increasingly using laptops, PDAs, Pocket PCs or even mobile phones to communicate with the systems back at the office. They may also want access, via the internet, from a client's PC or from a

computer in an internet café.

So, how do we guard against all the potential dangers?

### **A layered approach**

Most people agree that the task of securing computer systems requires a multi-layered approach but, essentially, it is no different from any other area of security, according to Gerhard Eschelbeck, chief technology officer and VP of engineering at Qualys. "When you look at IT security, it comes down to three aspects and the integration of them: people, process and technology," he says.

The people aspect concerns the training of staff, and determining the ownership of different parts of the systems. People need to know the name of their point of contact, their individual roles, and so on.

The process part involves the creation of a policy that is written down and then communicated, making sure that everyone within the organization understands the policy – that is, what it means to use resources, what it means to use the VPN.

Once those aspects are in place, the technology aspect can be tackled.

As Eschelbeck concedes, this has become a more complex task.

"Networks were once more simple, with a firewall connecting us to the outside world. There was a single point of access to protect," he says.

"Over the past years, networks have changed enormously. We have introduced wireless access points, and mobile workers can work anywhere on the internet. This is an extension of the

internal network out to the external network. We now need to protect those mobile workers."

Because the devices are outside the company's perimeter, they are unprotected – physically and logically, he says. "They have a different risk profile. There is the danger of devices being lost. There is also a danger when those devices are connected via hot-spots anywhere in the world."

Basic protection can be achieved on the device with three technologies installed: anti-virus, a personal firewall (to protect it from a networking and traffic perspective), and encryption of important files. "I recommend users install encryption technology on their mobile devices. It allows them to protect sensitive data and provide protection from the device being lost," he says.

### **SSL solutions provide flexibility**

For connection to corporate resources, there seems to be almost common consent that the new breed of SSL VPNs are ideal for the job. While IPsec VPNs are well suited for connecting branch offices in a secure way to provide seamless access to users, the SSL-based solution provides a good deal more flexibility. With no client software needing to be installed on the remote device, it means that users can gain

a secure connection from any browser-based device, such as a PC in an internet café or at a client's premises. The software creates a secure tunnel and encrypts the transferred data, thereby deterring snoopers from listening in.

Reggie Best, president and founder of Netilla, a provider of SSL VPNs, says customers appreciate the flexibility of the technology, but "they are now looking for new capabilities." He sees it as the start of what he calls the "secure

application access management marketplace," where organizations will be able to enforce security policies at a more granular level.

This means that the rights and privileges of any user would be determined not only by who they are, but also by the device they use to access the application, or from where they are calling. "If you are coming in from a corporate PC, you might expect to get a higher level of trust than if you are using an internet café," says Best.

That message is echoed by Jude O'Reilley, a marketing manager with rival VPN vendor Aventail. His company is also working on the provision of a more granular and centralized means of enforcing security policies for users adopting a variety of access devices. "It is part of a continuum to an unmanaged environment," he says. "It is a big challenge for IT security policy, because we have to provide access according to the user's risk."

Aventail's caution is well founded, according to Qualys's Eschelbeck. He says the flexibility of the SSL VPN could make some users careless. "It is wise to treat a PC in an internet café as an untrusted environment. These devices are not under your company's organization. You have no idea what is running on those machines," he says. You also have no idea what data you might leave on the machine that could be picked up by the next user.

### Updating security measures

The other key area he raises is the need to track mobile devices and ensure they are kept up to date. "It is important on an ongoing basis to look at new vulnerabilities and ensure users are properly protected," he says. "For example, with events such as Blaster and SoBig.F, for many it was already too late."

The SSL VPN, he says, is therefore "a double-edged sword," and his recommendation is that roaming users should always use a device that has been properly configured by the company's IT department.

"There is a challenge to keep a regular inventory of users' devices, and where they are roaming at any point in time. You then need to know what patch level they are at. That is not an easy task.

"Patching is not only a technology problem, it is also a people problem. We need to ensure people understand policies, when the patch needs to be applied, and when the IT department can distribute those patches out to the roaming workforce."

IT security comes down to three aspects and the integration of them: people, process and technology

**Gerhard Eschelbeck**, chief technology officer and VP, Qualys

His company's Qualysguard product goes some way to automating this process.

### **The user perspective**

Despite Eschelbeck's fears, many companies have eagerly grabbed the freedom offered by the SSL VPN.

Take Deloitte Consulting, for example, a global company with some 15,000 consultants in the field. They need to be out of the office earning fees, but they also require easy access to the Deloitte main systems.

"We work on the fundamental premise of people not being in the office," says the company's chief information officer Larry Quinlan, who says his aim is to provide his users with the most complete experience that security will allow.

The solution for him has been an SSL-based VPN device from Aventail which provides an encrypted connection into the corporate systems.

He believes the system works well, allowing consultants to work at a client's office and pick up mail from any PC with a browser. He uses both a client-less and client-based version of the Aventail system. The clientless version allows access from anywhere to certain systems, such as email, while those consultants who need full access to all applications systems will have the VPN client software loaded.

The only problem he encounters, from time to time, are those consultants who want to access systems while on

vacation." They'll come in from internet cafés in Jamaica, so we just ask them not to download attachments onto those kind of machines."

**Securing the endpoint as if it were its own corporate network is the required mindset.**

*Rag Wagner*, director of information security research, Gartner

### **Efficiency equals profit**

Another enthusiastic adopter of the technology is Dennis Brixius, CISO for industrial gases company Praxair. Not content with deploying his Aventail SSL VPN to the company's knowledge workers earlier this year, he is now forging ahead with a plan to put all 25,000 employees, including a fleet of truck drivers, on to the system.

"We think we can get a six-month return on investment with this system by cutting out all snail mail," he says. Instead of sending out notices to employees in the mail, Praxair will make them available through the VPN for people to access from home computers or any other device using a browser. He expects more calls to the helpdesk from users who have forgotten their passwords, but that has all been factored into the six-month ROI.

An interactive voice-response system will also keep down helpdesk costs by automatically answering user inquiries.

Brixius says the other great advantage of the SSL VPN is that it relieves most users

of the need to carry a laptop. Instead they can connect from any available PC. However, where users need to do some serious and confidential remote computing, Brixius still provides them with an IPsec-based virtual remote access system – less flexible, but more secure than using an internet café.

### **A security package is best**

The last word can go to Ray Wagner, director of information security research at Gartner, who sums up the task as follows: “I concentrate on the message that securing the endpoint (laptop, palmtop, whatever) as if it were its own corporate network is the required mindset. Centrally managed backup and data encryption, separately authenticated VPN (or no connection to the corporate network), strong authentication, anti-virus, and personal firewall would make up a minimum requirement for fairly strong mobile security.

“If you can’t provide the first, the machine should contain no mission-critical data (this is unlikely); if you can’t do the last four you have a hole in your corporate network. Even if the machine does not connect to the corporate network, anti-virus and a personal firewall are required for the health of the machine.”

*Ron Condon is editor-in-chief for SC Magazine.*