The Hidden Threat From Modem Access

Far from being an archaic and dying technology, modems continue to thrive. The risks they present go unnoticed and unchecked, resulting in an unsecured, publicly accessible data network that pervades all levels of an organisation.

The Security Dilemma

New technologies present opportunities for organisations to operate more efficiently, often in ways that would have been inconceivable only a few years earlier. Over the past decade we have seen widespread adoption of the Internet, wireless, and now Voice over IP. However, as each technology has been adopted, new risks have emerged – often after the fact, and often very publicly. One positive effect has been that both security and security awareness are probably further to the forefront than ever before. In part, this has been driven by stories in the mainstream media bringing these issues to the attention of the public.

The dilemma for any organisation is that when new technologies are adopted they tend to supplement rather than replace existing ones. The security burden therefore increases, but often without a commensurate increase in resources to deal with it. Inevitably, this leads to a prioritisation of effort. Typically this is in favour of the new technologies (they are more interesting, after all!) at the expense of older, more prosaic ones. One technology in particular is persistently overlooked. **Despite the broadband revolution, VPNs, two-factor authentication, and a whole host of other security advances, organisations are still open to a threat from a technology over a quarter of a century old: the humble modem.** It pervades organisations from all business sectors, of all sizes, at all levels.

Understanding Modem Access

To understand why, it's important to understand the specific roles that modems continue to fulfil. Before widespread adoption of the Internet, modem dial-up was the only practical means of enabling remote access. Whereas a dial-in gateway was often provided for users, support staff typically accessed IT systems directly through an attached modem. Fast-forwarding to today, most remote users access IT systems through secured network routes. However, for legacy systems (where integration into a modern security architecture can prove difficult), support staff may still require modem access. Equally, technical staff members have a habit of adding modems in an ad hoc fashion to key production and development systems, short-circuiting security controls.

The Infrastructure Challenge

Modem access to business systems is just the tip of the modem access iceberg, however. **Infrastructure systems** are where modems reign supreme. They are critical to business operations, encompassing everything from the network to the telephone system, faxing & printing, power regulation, heating and air conditioning. Only a few years ago, most of these functions would have been fulfilled by essentially passive, electronic devices. Not so today. Commoditisation of computer hardware permits manufacturers to procure off-the-shelf equipment far more cheaply than designing their own custom devices. One result has been a gap between perception and reality (reinforced by the manufacturers). Devices are often marketed as "appliances", with the robustness that this implies. However, they are anything but dumb. They are extremely capable, running complex computer operating systems (including Unix, Linux or cut-down versions of Microsoft Windows).

Such technological advances have undoubtedly provided beneficial for customers. Systems are inherently more capable, at a far lower capital cost. Furthermore, the intelligence built into these devices allows them to be managed remotely, providing better management at reduced operating cost. Typically, systems will be accessed through an installed modem, directly connected to the outside world via the public telephone system. Indeed, for standalone or remote devices, or components of network infrastructure, a modem may provide the only practical solution for remote management.

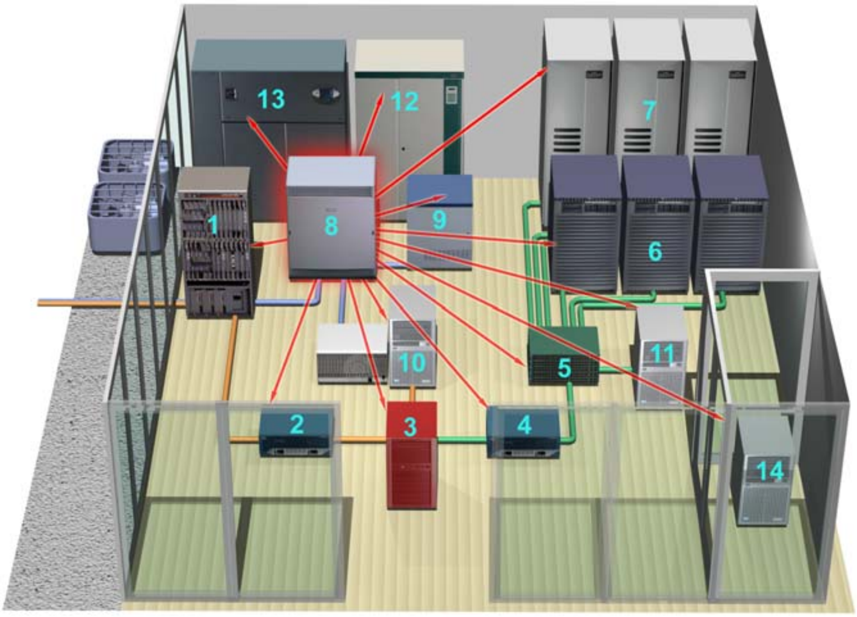
Why Existing Security Controls Just Aren't Enough

Clearly, access to infrastructure systems needs to be secured – after all, your business depends on them. The first common misconception is that your firewall will take care of it. It won't. A modem provides an access route that completely bypasses the firewall. Nor will any intrusion detection systems be of any use. Paradoxically, even without these protections, remote dial-in access can provide a cost-effective and secure remote management solution. Unfortunately, it is often neither sufficiently well managed, nor monitored to achieve these goals. At the same time, scale becomes an issue. Uncontrolled, modem access proliferates to an alarming degree. **We commonly detect 0.5 – 1.5% of <u>all</u> an organisation's telephone lines providing dial-in access to a modem – amounting to hundreds of unpoliced routes in a large organisation.**

The perils posed by unrestricted modem access are well documented and understood. Both BS/ISO 17799 and the Payment Card Industry (PCI) Security Standards make recommendations on how it should be managed. Rightly so. According to UK DTI-sponsored research, unsecured remote access is one of the routes most-favoured by hackers.

Given this background, it might be reasonable to expect that modem security would be near the top of the security agenda. It isn't. It's the new threats that hit the headlines, and garner most

The hidden data network accessible through your telephone system…



1	*Voice/data bandwidth manager*
2	*External router*
3	*Firewall*
4	*Internal router*
5	*Network hubs/switches*
6	*Application servers*
7	*Disk arrays*
8	*Telephone PBX*
9	*Voicemail System*
10	*Remote Access Server*
11	*Authentication server*
12	*Uninterruptible power supply*
13	*HVAC (air conditioning)*
14	*Building access control system*

attention. Modems are largely hidden, both from sight and from mind. Although they shouldn't neglect the more prosaic risks, that's exactly what most organisations do. According to the same DTI study, **in 2004, only 8% of large UK organisations audited for dial-in modem access.**

Modems & E-Crime

Unsecured modems present an especially attractive target for cyber criminals. Attached to key computer systems, they present opportunities for direct monetary gain and for propagating identity theft. Attached to telephone and voicemail systems, they present opportunities for toll fraud. What we shouldn't forget, however, is that there are motivations other than money. Access to key elements of infrastructure presents an opportunity to inflict malicious damage by disrupting business operations. *Insiders* are often cited as presenting the biggest risk to an organisation's security. Who better to install a rogue modem, or know where they are or how they are configured?

What makes a modem-initiated attack even more attractive to a malicious hacker is the fact that it is likely to be untraceable. Whereas most organisations monitor outgoing calls as a means of controlling call costs, our experience is that very few monitor incoming calls. Consequently, the early signs of an attack (such as call activity at unusual times) are likely to be missed, and it will be difficult to impossible to trace afterwards.

Fear, Uncertainty, Doubt… or a Real Problem?

Financial losses directly attributable to unsecured modems are difficult to quantify. Modems are hidden; attacks occur "in private", with little incentive for organisations to report this type of breach. There is, however, one clear incentive for investigating how the issues surrounding modem access might affect you: the financial investment in security technology that modems undermine. So, to discover if they apply, simply pose a few questions:

- ❑ Does your security policy restrict modem access?
- ❑ Are authorised modems always configured in compliance with policy?
- ❑ Do you have any unauthorised modem access?
- ❑ How do you know?

The chances are that no-one in your organisation can give you a definitive set of answers.

Because, statistically, there's a 90% chance no-one has looked.

For more information, contact

Xiscan Limited
9 Old Hall Farm
Brickwall Green
Liverpool
L29 9AF

T: 0870 011 8075
F: 0870 051 8062
W: www.xiscan.com
E: info@xiscan.com