Alternatively, if the site is configured to use SSL, this can be used to encrypt the authentication exchange. There are other authentication options, but they rely on the site users and the Web server being part of the same NT domain — fine for an intranet, but not applicable to public websites.

Secure users

Monitor use

Finally, you need to check continually that nothing is going wrong, and for this you need a site log. IIS writes access logs in a configurable variety of formats, and the default format is easy to read with any audit software.

The usual trouble is that if the Internet connection is mediated by a firewall, often the only IP address that shows in the logs is that of the firewall itself — in practice, the firewall log may be a better place to look for hacking attempts.

This is an important area, often neglected. If you pay attention to the site security, you reduce your chances of a successful hacking attempt, but you don't guarantee it. Someone needs to review the logs regularly, to check that nothing untoward is being attempted. The skill in doing so is to select what to review in an intelligent way, and then automate the reporting as far as possible. Administrators tend to complain that reviewing the logs takes too much time: but I've seen some excellent examples of reporting set up to operate to a schedule, where the administrator has to do no more than review a short email every day or every week. This provides excellent assurance that all is well — and should give advance warning of potential hacks.

Conclusion

The business objectives for the Web server may be unusual: but a technical audit plan for the server shows us a list very similar to the one we'd have for a standard application. The key areas are:

- Control of Web server administrator access;
- Correct setting of the NT and IIS access permissions;
- Correct settings for user access and authentication;
- Informative logging which is regularly reviewed.

Thus the audit has strong similarities with other technical computer audit areas. One difference you may find is that security may have been neglected in the rush to get those Web pages online: so your work can make a real difference in highlighting risky areas.

About the author

Alison Webb BA FCA MBCS CISA has been an independent computer audit consultant since 1990. Her telephone number is +44 01223 461316.

Crying 'Havoc', Crying 'Wolf' or Just Howling at the Moon?

Matthew Pemble, IS Integration Ltd

I had thought of several other names for this article: "Chicken Little in the IT undergrowth" and "The Computer Security Company that cried: 'The End of the Internet'," so you can probably already see where this article is going. A less entertaining, but probably far more descriptive and appropriate, title might have been "Responsible Behaviour in an Irresponsible World." The computer industry is beginning to get a public reputation for producing horridly doom-laden statements which turn out to have no basis in reality. Please note, this is my opinion of the public perception, not an appropriate and accurate analysis of the truth.

The massive hype for the third Code Red "outbreak" on 1 August, fuelled by the Microsoft, NIPC, CERT, SANS and others joint public announcement only enforced this long-term trend, which started *well* before Y2K.

By the end of the day, there was quite a considerable amount of Code Red traffic flying around. This did cause some problems and significant clean-up costs to many organizations, even before Code Red II, with its far more dangerous payload (admin level remote shell access,) appeared.

However, the stories that had appeared in the press in the run-up to the date-change insisted that: "the end of the world is upon us." As the events of 11 September, as well as natural disasters around the globe, have made entirely clear to us that you cannot rationally equate communications network failure with tragedy.

If the entire Internet disappeared permanently tomorrow, the world would recover, probably remarkably quickly. I would probably have to join Gene Schultz's "12 Point Plan" for stopping consulting, but things would get back to some version of normal.

What can be done to prevent us sliding into public disbelief and ridicule? We do know that there are ways to create situations where information security failures can cause real-world damage: IP enabled medical equipment on Internet connected LANs and power generation and supply control systems being obvious examples. Financial services and retail bank systems failing could cause significant upset or even personal misery. Bad systems design, especially with ERP systems, has caused corporate bankruptcy, with ensuing worker lay-offs and consequential impacts on associated organisations. We need the credibility that when we point this out, we are believed by management, regulators or the public at large.

What to do?

There is a very serious issue here. The UK Government has passed the Private Security Industry Act into law. The Department of Trade and Industry is now, after the fact, "consulting" in an attempt to deal with the registration and licensing of the information security industry already enabled by dangerously loose[1] legislative wording.

The Digital Millennium Copyright Act contains numerous exemptions from its more dictatorial provisions, for (and this is a paraphrase) "appropriate practitioners". Even in the heart of the security community, at the COSAC 2001 conference, there were suggestions that we should become a "profession", with all of the licensing and regulatory implications that involves.[2]

My personal opinion is that government directed licensing would be fundamentally damaging to our independence and that any conceivable implementation of the lesser evil, legislated professional registration, would not successfully encompass the diversity of backgrounds and competencies that is one of our industry's main strengths.

I think that there are significant things we can all do and, more importantly, that we are professionally responsible for seeing that they, or something similar, come to pass.

Beware of the media

Firstly, we need to be careful when talking to the mainstream media. Even the technology correspondents of the national press are journalists first and foremost. The technical ignorance of the vast majority of the reporters I have spoken with is simply staggering. We must remember that their key interest is getting a story that looks good in print, not necessarily in getting the technical details accurate.

They are also very bad at dealing with honest ignorance — having dealt with so many politicians, I suppose, they treat equivocal responses as malicious withholding of information. We must also remember that we should be careful of using the experience to promote our products. Most journalists have very well-tuned 'marketing' detectors. If your company manufactures or sells a product or service that helps alleviate whatever you are discussing, make that statement, but please do not link your entire answer or commentary to your organisation.

Red alert

Secondly, we need to be very clear when we draft vulnerability announcements or security notices. This is not a demand for people to end full disclosure of vulnerabilities, or even for "responsible disclosure". I believe that the arrogance and systems engineering incompetence of so many software vendors requires full disclosure (although I wish it was not necessary).

However, if you are ever in the position of having found a new problem and, as seems to be usual, the vendor is refusing to talk to you because you do not have a support contract, does not answer your emails, or simply does not believe you, you have a duty to explain yourself properly.

Detail which systems you have tested and which you have not (and why, if you think it important). Be precise when stating which systems were and were not vulnerable.

The Microsoft .ida warning, MS01–033, is a wonder of muddle and confusion, obscuring (mostly) correct information. Look at the title and affected software lines: "Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise" and "Index Server 2.0 and Indexing Service", respectively.

Both of these most strongly suggest that either Index Server 2.0 or the IIS 5.0 Indexing Service have to be installed for you to be vulnerable. As we know, this is not true, and PWS, IIS 4 and IIS 5, as a default, *all* install vulnerable versions of the idq.dll file. When I first wrote about this, I was set to damn Microsoft for issuing an incorrect bulletin. However, the first line of the actual bulletin "Issue" section is actually completely correct:

"As part of its installation process, IIS installs several ISAPI extensions — .dlls that provide extended functionality. Among these is idq.dll, which is a component of Index Server (known in Windows 2000 as Indexing Service) and provides support for administrative scripts (.ida files) and Internet Data Queries (.idq files)."

Apart from not mentioning PWS, this does make it clear that all you need is to install IIS, 4 or 5, for the vulnerable dll to be installed on your system. However, even a security specialist (and I'll blame the huge daily volume of my email which lands in my inbox for the mistake), made a completely incorrect assumption. Mea culpa. Hard on the brain though it is, I'll read them more fully in future.

Risk management

Thirdly, in your organization or at our customers, we need to encourage the process of proper business and technical risk management. Sit down with your (or their) bosses to work out what loss of, say, all email services for two days (under a virus attack, for example) would actually cost the business in hard cash. Make this process part of your regular system reviews. The long term benefits of proper risk assessment and management will easily outweigh the minor inconveniences of another meeting with the boss.

Contrast that with, as another example, losses incurred if customers could not access your main corporate website for a day or possibly a major breach in customer confidentiality. The marketing department, who have to do this sort of educated guesswork every day, targeting resources in

[1] Although, to break the habit of a lifetime and be fair to a government department, it was the Home Office who drafted the Act, not the DTI.

[2] I speak as a fully licensed and appropriately regulated professional engineer.

the hope of increased sales, should provide a good data — from a source the business managers are used to accepting. Remember that the losses that you will suffer should this sort of breach happen will last a lot longer than the period of downtime. Your reputation may suffer considerably and for a protracted period.

Luckily, formal, documented risk analysis need not be a lengthy or difficult procedure. It will require you to get together suitable representatives from every stakeholder, but there are tools and guides to help you.

A word of warning, however. Beware tools which ask too many closed questions: use less technology and more brainstorming or lateral thinking. Reject, out of hand, any tool which gives you a magic answer whether acceptable or not acceptable risk, or the even more dangerous "numerical risk value". No out-of-the-box tool can provide you with the insights people within your company have. It is conceivable that with sufficient time away from your real job, you could write or modify a tool so it would give you a compliance correlation with your corporate security policies. However, breach of a security policy or control is not, of itself, a complete and proper determination of unacceptable risk.

The business of most organizations is the acceptance of risk in the search for profit or achievement of business objectives. Put simply, we trade risk against the need to raise profits. Managers just need sufficient relevant information to make properly informed decisions.

Lastly, and this is by far the hardest, we need to start sharing security information. Not, of course, the nasty detailed stuff about the admin accounts "gtx" with password "gtx"[3], or the IP addresses of boxes with unpatched Web servers. What we actually need is comprehensive information on the use of vulnerability data actually to exploit systems. I am thinking of something along the lines of the airline industry and their anonymous notification procedures for incidents.

Sharing this sort of information with a trusted third part who we could all rely on to collate and feed information back would improve both awareness and vendors ability to address emerging issues. For this we would need to choose somebody reliable and trusted: SANS or SecurityFocus, for example. As part ~of the existing GIAC or ARIS services, providing proper incident analysis and advice, maybe you could be allowed to submit completely anonymous reports. This would allow (as proper as we are going to get) statistical analysis of what the various hackers and hacker groups are *actually* using to break into machines. From that, we could really determine true threat levels and start providing the business with hard data. Accepting, of course, the problems of the "self selecting sample" in providing the statistics, but that applies just as significantly to the annual CSI/FBI survey.

There are going to be a very large number of hurdles to overcome, not least business objections to allowing any information about security breaches outside of the organization. With Hushmail, Zero-Knowledge protocols, and other anonymous systems, these problems have, to a certain extent, been solved technically. Although of course it would probably take a few years to gain the trust of some companies, particularly those who perceive themselves as being in a high risk category. Getting such businesses to comprehend the advantages of such a system, however, be a problem of a different magnitude. Nevertheless, if we do manage it, we might actually get to be able to manage some degree of prediction. The combination of Netcraft's surveys[4] and statistically reliable knowledge of how far how many people are behind with their patches are such useful tools. Then we might be able to predict how we could react to new detected or proposed threats.

Consider the "evolution" of proposed worm designs, as a result of the detailed metrics of Code Red spread and correlation of those to code (mostly PRNG) characteristics. There are very few systems that couldn't be shut down safely in the 16 hours Code Red took to play out. You might even be able to patch systems before you got hit and stay online, more or less. If you had a central warning system that spotted the problem first, you would have a headstart on implementing a solution so you wouldn't have to impact performance or productivity during business hours.

The Warhol worm, giving you fifteen minutes, should allow you to run down to the computer room and pull the network cable out. Stuart Sandiford's flash worm, running through in about 30 seconds, is barely going to allow you to put down your cup of coffee.

Vulnerabilities will come and they will go. We will patch them (or at least some of us will) and we will wait for the merry-go-round to circle once more. I am afraid that the dramatic and automated exploitation of these vulnerabilities will only increase.

We, the security community are guilty of burying out heads in the sand as far as patches. But our duty goes beyond this. By drawing out pay packets we have accepted a comprehensive duty to our employers and clients, and a general duty to society, to conduct our affairs in a professional and responsible manner and to take positive actions to ensure that future security breaches are prevented wherever possible. We must eschew hype and FUD[5] in all their forms, rein in the wild horses of the media, and refrain from self-publicity at the expense of technical (or business) accuracy. If we don't, not only is our industry at risk, so may be many people's livelihoods or even, in extreme cases, people's lives.

[3] You know who you are!

[4] Though I do wish they would start up looking at ports other than 80 and 443! I would love to see relative BIND, M$ DNS and DJBDNS statistics.

[5] Fear, Uncertainty and Doubt