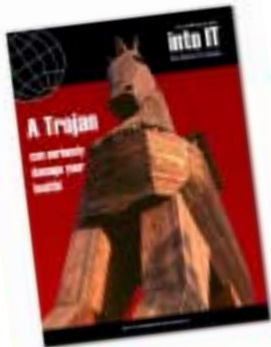


into IT editorial



intoIT is the journal of the INTOSAI Standing Committee on IT Audit. The journal is normally published twice a year, and aims to provide an interesting mix of news, views and comments on the audit of ICT and its use in Supreme Audit Institutions (SAIs).

Material in the journal is not copyrighted for members of INTOSAI. Articles from intoIT can be copied freely for distribution within SAIs, reproduced in internal magazines and used on training courses.

The Editor welcomes unsolicited articles on relevant topics, preferably accompanied by a photograph and short biography of the author, and short news items for inclusion in future issues.

The views expressed by contributors to this journal are not necessarily those of the editor or publisher.

editorial address

Contributions should be sent to:

The Editor of intoIT
National Audit Office,
157-197 Buckingham Palace Road,
London
SW1W 9SP
United Kingdom

E-mail intoit@nao.gsi.gov.uk
Web site www.intosaiitaudit.org

New legislation before the U.S. House of Representatives requires all publicly quoted companies to conduct independent, computer security assessments and report the results in their annual reports. The Corporate Information Security Accountability Act of 2003, if approved, requires companies "to assess the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems," and "determine the levels of information security appropriate to protect such information and information systems".

The Act requires companies to hire an independent auditor to assess existing information security controls and ensure that they meet basic standards that the U.S. Securities and Exchange Commission has yet to determine. It will be interesting to see whether the standards will also extend to the independent auditor's qualifications and experience for reaching a meaningful and reliable conclusion. Is the auditor likely to be a thoroughgoing, information security professional, or a financial auditor who has completed the (5-day, or whatever) course? Will the audit merely confirm the existence of the right documents - suitably dated and authorised - that say the right sorts of things? Or will the auditor be required to conduct more searching tests to assess whether the documentation is a façade that, in good 'cowboy town' tradition, is propped up by nothing more than a few scaffolding poles? And will organisations who, having acquired the auditor's seal of approval, rest complacently on their laurels for the next 12 months? We await developments with interest.

A recent prime-time UK television programme featured real-time burglary. An ex (so we were told) professional burglar was hired by the programme producers to break into the homes of volunteers and 'borrow' their valuables. It was disturbing to witness the ease with which our resident expert generally accomplished his task. Truly, "penetration testing" in the raw.

Entertainment aside, there was much to learn from the ensuing debate, which considered the vulnerabilities uncovered and the countermeasures that ought to have been in place¹. Door and window locks, security lights and their positioning, intruder alarms, and a host of other techniques were examined and discussed. Household security was then strengthened and retested, and while the improvements did not always withstand further attack, an important point emerged. *Potential intruders are deterred by effective countermeasures* because their penetration is time-consuming and likely to attract unwelcome attention. The trade much prefers soft targets from which, it seems, there are plenty to choose.

Although this scenario relates to the real world, it maps easily onto cyberspace, where network administrators have daily to pit their wits against increasingly sophisticated intrusion techniques. As IT systems become increasingly interconnected, more national and global networks are emerging, and while this opens up unprecedented opportunities and benefits for both citizens and state alike, it presents the criminal with new opportunities. Systems connected to the Internet and to other networks become potential targets and the high level of attacks against commercial and government systems, as well as

¹ See . . . <http://www.bbc.co.uk/crime/prevention/yourhome.shtml>

contents

individuals, continually demonstrate the skill and determination of cyber criminals to exploit technical vulnerabilities and human naivety. There can be no doubt that, as more business is transacted online, the potential for cyber crime and its incidence will increase. Although most network administrators take sensible precautions, they have other responsibilities and cannot always be blamed if they are not abreast of the latest, often highly ingenious, technical exploits that facilitate cyber crime. This is work for the specialist, and it is here that well planned and conducted penetration testing can expose serious vulnerabilities.

In this edition we highlight some of the technical and procedural countermeasures for protecting networked information systems, including penetration testing, a technique that despite its risks is becoming a more widely accepted strategy for protecting online information and services.

Our first theme article provides a layman's guide to hacking. For the benefit of readers who are unfamiliar with the subject, N. Nagarajan of the Office of the Comptroller and Auditor General of India explains some of the approaches to computer hacking and the terminology that often crops up in connection with it.

Our second theme article describes a penetration-testing project that was planned and supervised by the Office of the Auditor General for North Carolina. The article is interesting both for its description of the outcome (21 of the 22 target systems were penetrated successfully, most in less than 30 minutes) and for the approach to the task.

The focus of network security used to be at the perimeter, where firewalls were positioned to keep uninvited guests



out of the internal network, but growing recognition of the risk of attack from within and the advent of e-mail as a vehicle for planting a Trojan in the system has changed the picture. Our next three articles develop this theme. Written by staff at the UK's National Infrastructure Security Coordination Centre² they provide an overview of recent developments in intrusion detection systems; of e-mail spoofing, a technique sometimes used by hackers to obtain system passwords; and of Trojan horse software. And believe me, a Trojan can seriously damage your health!

To round off this edition's theme of hacking, we have received an excellent article from the Auditor of Public Accounts of the Commonwealth of Kentucky, USA. Ed Hatchett takes a robust stance on the subject of network security, commissioning detailed technical appraisals of state departments' controls and not being shy about publishing his findings. In his article, Ed describes the results of an audit of the Transportation Cabinet network in which his team uncovered both hackers at work and criminal activity. And yet top of his recommendations is the simple expedient of applying a good standard of password management.

² NISCC's role is to co-ordinate and develop the UK critical national infrastructure's defences against electronic attack... <http://www.niscc.gov.uk>

Country Focus:
The UK National
Audit Office

2

Not Knowing What
You Do Not Know

12

State of
North Carolina

20

Trojan Horses and
Kernel Root Kits

24

Intrusion Detection V
Intrusion Prevention

26

Email Spoofing

29

A State Auditor's Network
Security Case Study

31

Risk Based Sampling
Using COBIT

36

Going Electronic

40

Freedom of
Information

43

Dig the Spacedirt

48

GAO Working
with Congress

51

A Chilling Thought!

55