Cybercrimes o

Security holes in Windows NT make it an easy prey

By Safdar Hussain

THE soaring rate of crimes has been a cause of severe headache for administrations around the world at all levels. From governments to organizational watchdogs, they have all worried about how to reverse the trend. Indeed, they would be very happy just to stop it at whatever level it is right now. Under such circumstances, one can well imagine their disgust at checking incidents that now comprise the field of cybercrimes.

In February last year, hackers launched and distributed denial-of-service attacks on several prominent websites, including Yahoo, E*Trade, Amazon.com, and eBay. Some eight months later, Microsoft reported that hackers had tapped into the digital blueprints of the company's future products, highlighting the major information security risks that plague an increasing number of Global 2000 (G2000) companies with no formal policies and weak or disorganized security measures and controls.

According to recent survey data recorded in the United States, nine out of ten companies and government organizations reported security breaches in the past one year. Of the 42 per cent willing to quantify the damages and financial losses, the total ran to $265 million.

As Internet commerce continues to soar, cybercrime is increasing exponentially. The Department of Justice caseload reflects this growth. In fiscal year 1998, it opened 547 computer intrusion cases; in the 1999 fiscal, the number jumped to 1,154 (up 53 per cent). Similarly, the number of pending cases increased from 206 at the end of fiscal 1997 to 601 at the end of fiscal 1998, to 834 at the end of fiscal 1999, and to more than 900 by middle of fiscal 2000 (a 77 per cent increase in pending cases in less than a three-year period).

And these are only the reported cases. Experts believe that at least 50 per cent of cybercrimes go unreported due to the potentially adverse publicity, embarrassment and negative effects that such disclosures would have on consumer and investor confidence. In fiscal 2000, the US Congress appropriated an additional $37 million for fiscal 2001 for the Department of Justice to expand its staffing, training, and technological capabilities to continue the fight against computer crime.

Together, these enhancements will increase the Department's funding base for computer crime to $138 million, an increase of 28 per cent over similar funding for the fiscal 2000. As more companies continue to embrace the Internet commerce channel, we believe the private sector will see similar funding increases for information security controls and programme costs, ranging from a 10 to 20 per cent increase during 2001-02 to a 25 to 30 per cent increase by 2003-04 over current spending levels.

Currently, only five per cent of G2000 CIOs have linked IT policies with business policies. By 2002, more than 50 per cent of G2000 firms will have stated business policies, and by 2003, more than 50 per cent will have linked IT policies that integrate with the business model and policies. A glance over what is being reported by

Issues

newspapers and specialized magazines across the United States suggests that a vast majority of experts in the field believe that by 2002, more than 50 per cent of G2000 companies will adopt enterprise-wide information security policies, and that by 2003-04, this number will be more than 75 per cent. Given that there is an increase pattern in risk and a corresponding increase in defensive spending to address cyberrisks, CIOs should have an understanding of security policy development best practices.

Highly effective CIOs base their enterprise-wide information security policies on the results of a risk assessment, which provides them with an accurate picture of the security needs specific to the enterprise. IT security risk assessment information is imperative because proper policy development requires managers and decision-makers to undertake a serious exercise.

It involves identifying sensitive information and critical systems; incorporating local, state, and federal laws, as well as relevant ethical standards; defining institutional security goals and objectives; setting a course for accomplishing those goals and objectives; and ensuring that necessary mechanisms for accomplishing the goals are in place.

In this way, legal and regulatory concerns, organizational characteristics, contractual stipulations, environmental issues, and legal input could all be incorporated into policy development. Effective security policy synthesizes these and other considerations into a clear set of goals and objectives that direct staff as they perform their required duties.

Formulating policy is usually a task reserved for top-level decision-makers (corporate, executive policy committees); however, contributions to the development of information security policy should be an enterprise-wide activity. Though every employee does not need to attend each security policy planning session, the CIO and senior management should assign representatives from disparate job levels during the information-gathering phase.

IT technical, administrative, and operations staffs have a unique perspective about information risks and controls to share with policy-makers. The CIO should task the head of the IT information security department to gather input from all parties to ensure there is buy-in at all levels of the enterprise.

Reviewing security arrangements in other organizations might uncover information that can contribute to more effective policy development. In a B2B arrangement, if one or more parties commits to specific encryption policy and software to protect messages and transactions sent over the Internet (and the other B2B partners on the network do not have the encryption keys), they are going to have a very difficult time communicating with their e-commerce partners.

Though an organization's risk assessment informs a CIO of the specific security needs, the following general questions should be addressed clearly and concisely and reviewed by the CIO prior to submission to the corporate policy committee:

What is the reason for the policy?
Who developed the policy?
Who approved the policy?

n the rise

o hackers around the world

Whose authority sustains the policy?

Which laws/regulations (if any) is the policy based on?

Who will enforce the policy? How will the policy be enforced?

Whom does the policy affect?

What information assets must be protected?

Who is the information owner (best source for shared information)?

Who is the custodian of the information?

Who decides who reads, creates, modifies, stores, distributes, or deletes the data?

What are information users required to do to safeguard the data?

How should security breaches and violations be reported? And how often?

What is the effective date and the expiration date of the policy?

Effective CIOs will absorb these recommendations, as appropriate, and communicate the results into a meaningful governance policy that fits the enterprise.

By adopting these standard procedures, several commercial firms in the US have reported success in their efforts to control the menace of hacking. And the trend is catching on.

Meanwhile, a survey has recently been posted at Attrition.org, a site that celebrates the exploits of hackers and points out the security holes of established companies. It talks about organizations as diverse as NASA, the Communications Workers of America and Palminfocenter.com, the common ground among them being the fact that each of them had its website all defaced at different times last year by a hacker using a security weakness in Windows NT, the precursor to Microsoft's Windows 2000 server software.

Those episodes, along with the embarrassing hack of the software giant's own corporate networks, probably helped Microsoft's Web server software win the title of most vulnerable to hackers.

Of the defacements in December, 57.98 per cent came on servers running Windows NT, while those using Windows 2000 were tallied at 9.96 per cent. The servers running the Linux versions accounted for just more than 21.3 per cent during December. Sun Microsystems' Solaris saw about 4.1 per cent of the defacements.

Overall figures for defacements from August 1999 to the present peg Windows NT at 56.69 per cent. Windows 2000 came in at 2.41 per cent, but the software, an upgrade to Windows NT, launched on Feb 17, 2000, about six months after the beginning of the period covered by the statistics. Combined Linux defacements over this period were steady around 21 per cent.

Why is Microsoft a target? "I think Microsoft software is actually a target because Microsoft is so powerful and popular that anyone who succeeds in breaking into that software usually gets a lot of interest in the press," Dan Kusnetzky, a software analyst, has been quoted by the IT-related US media. "Many of these people are hacking because they want to be known."

The company's software is also the most commonly used, leading to inflated numbers of hacker attacks compared with other platforms. Windows NT is believed to be holding about 38 per cent shares of the shipments of server software in 1999. Linux captured a 24 per cent share of shipments, Netware held 19 per cent, and Unix had a combined market share of 15 per cent.

Another reason Microsoft's software may be a favoured target is the company's alleged propensity toward focusing on ease-of-use and on the time it takes to develop an application and get it shipped. "There is a trade-off if you make it very easy to develop applications to deploy them; sometimes you may take some shortcuts in security," Kusnetzky said. Still, security experts agreed that the methodology used by Attrition.org needs to be studied more closely before drawing any conclusions. "What this shows us is that all systems continue to have security problems," said Matt Bishop, an associate professor of computer science at the University of California. "That is why we are all banging our heads against a wall."

That be the case, organizations with their affairs conducted in a computerized environment need to be on their toes. Short-cuts can only lead to disasters, they need to realize before it is too late. ❑