

Network Security in Vietnam: Improper Attention

Posted: Friday, April 03, 2009



The Security World 2009 Conference and Showcase has recently jointly held in Hanoi by the General Department of Technology under the Ministry of Public Security, the Vietnam Computer Emergency Response Team (VNCERT), the Ministry of Information and Communication and IDG Vietnam. Lecturers and specialists saw a panorama of data and network security in Vietnam. Arguably, the computer viruses hacker attacks caused serious harms but the investment for protection and prevention seems inadequate.

Reality

In Vietnam, the cyber world has gradually become a virtual society, implying lots of security risks. According to Department of Information Technology under the General Department of Technology of the Ministry of Public Security, commonly known as E15, numerous security vulnerabilities existed in Vietnam, with nearly 60 million computer infections and 461 website hacks, including 251 incidents international hackers in 2008. Besides, more than 40 cases involving hi-tech criminals caused a loss of VND30 trillion. According to the Bach Khoa Internetwork Security Centre (BKIS), virus strain soared five times higher than in 2007 while dozens of websites were attacked each month.

Mr Nguyen Tu Quang, Director of BKIS, said “After two silent years, IT crimes have come back. The specific instances include the attacks to PA Vietnam, Techcombank and DDos. Last year, the outbreak of virus was regarded as a remarkable concern in Vietnam as malicious code booms on daily basis. Apart from the proliferation of viruses, the applied technology for virus production and malware distribution has been growing rampantly. Virus coders have been engaging increasingly in fraud and black-money making.”

Mr Nguyen Viet The, Director of the Department of Information Technology under the General Department of Technology of the Ministry of Public Security

According to McAfee, in 2008, companies worldwide lost about US\$1 trillion due to intellectual property

ty, said: hi-tech criminals in Vietnam had increased in both scale and severity. The targets of hi-tech criminals are not only database of financial companies, banks and emails but also information systems of State organs.

Mr Nguyen Anh Tuan, Director of Planning, Research and Development Division under the Information Technology of the Bank for Industry and Trade of Vietnam (Vietinbank), said: The core reason for the increase of hi-tech criminals in finance and banking sector was improper protection for greater numbers of online transactions. In another angle, the increase of online cheats in Vietnam and the world has the same reason: improper control and prevention.

Clearly, the target of hi-tech criminals in Vietnam is the money. Thus, the number of illegal accesses to websites and servers to steal personal information and credit card information used for international trading is soaring. Their targets are the database of the national information infrastructure, banks and big companies. They use phishing, trojan horses, spywares, key loggers and adwares to steal email, credit card information and personal information like name, address, telephone number and social security number. They even forge credit cards to withdraw cash from ATMs and colour cards to pay for other services and transfer money from stolen accounts to e-money accounts in e-gold and e-passport.

According to Tuan, institutional and individual users as well as news agencies are not fully and clearly aware of hi-tech criminals. In fact, most incidents were caused by low-rankings which use the hi-tech to proliferate and spread toxic behaviours quickly and easily.

According to surveys of VNCERT, based on international standards, 40 per cent of respondents had no firewall, 70 per cent did not set up any security disaster recovery system, and 85 per cent of enterprises did not have any information security strategy.

Forecast for 2009

Specialists thought that the deepening global economic recession will abet new attacks targeted at network systems and data of finance, banking and online payment institutions for illicit money taking. Amid recession, many companies will cut investment and staff and to launch more advertisement programmes on the internet environment. According to many specialists, the development of e-commerce will become a new target of technological crimes.

Despite mounting concerns over the increasing presence of viruses, Mr Quang of BKIS is confident that the situation will be better if China enact its amended Criminal Code soon. Accordingly, virus proliferation to steal information or illegal access to computers in the world's most populous nation will face very strict punishments. Then, the number of global viruses is expected to drop dramatically as a large majority of dangerous codes are now originated from China.

Experts forecast that attacks and hacks are likely to decline because violations have been strictly punished. The trend will be clearer after the amended Criminal Code will be ratified by the National Assembly in early 2010. Provisions involving hi-tech crime have been collaboratively compiled, amended and supplemented by the Ministry of Justice and the Ministry of Public Security. Expectedly, definitions of violating behaviours like service refusing attack, virus dissemination, cheating and online attack are very detailed. The highest penalty is 12 years in jail. This is the legal corridor to treat violations of hackers in Vietnam.

theft and Information System damages. Three main reasons for data leakage and system breach are: cost cutting caused by neglect of security system; growing attacks of hi-tech criminals and corporate insiders. McAfee forecasts that the tightening economic context will accelerate data theft incidents in 2009.

Urgent security investment

Computer virus leaves the most direct impact on and enormous damage to users. Thus, it needs special priority. Comprehensive computer virus prevention solutions on the market are ready for enterprises. The matter is the enterprises need to be familiar with using copyrighted antivirus software and technical support from producers. Virus killing is then very simple.

To ensure corporate network security, administrators must have security designs for both software and hardware. In operation, patch update and network hole checking must be regular activities. However, to apply a comprehensive corporate security solution, according to Mr Quang, users should adopt ISO 27001 certification standard. The ISO 27001 is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). The principle of ISO 27001 is to determine the organization's risk exposure/profile, and identify the best route to address this. The document produced will be the basis for the next stage, which will be the management of those risks.

Mr The also asserted that the network and data security is of a special concern. He said organisations and companies should consider proper investment for this matter in spite of trimming costs. At the national level, it is essential to form an organisation responsible for conducting researches and push forward technical proposals to deal with bad behaviours on the internet, he noted. Such an organisation should have the presence of responsible ministries like the Ministry of Information and Communication, the Ministry of Public Security, the Ministry of National Defence and other bodies.

Nguyen Thoa

http://vibforum.vcci.com.vn/news_detail.asp?news_id=16062&parent_id=0&cate_id=5



Effective IT security strategy needed

The 2009 Security World Conference and Exhibition opened in Hanoi on March 24, attracting a large number of leading information technology (IT) experts, senior government officials, policy-makers and businesses operating in the field.

The two-day event, themed “Secure your organisation in an insecure era”, was jointly held by the General Department of Technology under the Ministry of Public Security (MoPS), the Vietnam Computer Emergency Response Team (VNCERT) under the Ministry of Information and Communications (MIC) and the International Data Group in Vietnam (IDG Vietnam).





The conference discussed the hottest issues on information security during the current economic downturn. In a volatile economy, enterprises face a greater security threat, from cyber crime attacks to the theft of valuable corporate information. The vital question for organisations is how to create an effective strategy for the security of information that can ensure business continuity within a limited budgets.

Addressing the conference, MoPS Vice Minister Dang Van Hieu said that

Security World '09 will seek out solutions and technology for public security and national requirements in security fields such as networking security, data protection, surveillance systems and hi-tech crime prevention.

"The event has become a prestigious and high profile forum for IT experts, chief executive officers (CEOs) and chief information officers (CIOs) from governmental institutes and enterprises," he said.

The event highlighted critical issues in the National Information Security Strategy and Technology Platform for Public Security, regarding the law, data encryption standards and cooperation with the national information security authority.



Deputy Director of the Department of Financial Informatics and Statistics, **Tran Nguyen Vu**, said that the conference is taking place in the context of cuts in IT budgets and security spending due to the pressure of an economic downturn.

"The information security strategy encompasses security policies, compliance controls as well as solutions at both local and network levels", he noted.

According to McAfee (2009), companies worldwide lost nearly US\$1 trillion due to

intellectual property theft and damage to information systems. The three main reasons for leaked data and system breaches are: cost cutting and the negligence of security systems; growing attacks by hi-tech criminals and corporate insiders. McAfee forecasts that the tightening global economy will increase incidents of data theft.

The MoPS said that numerous security vulnerabilities exist in Vietnam and nearly 60 million computers have already been infected by viruses. There were 416 incidents of website hacking and international hackers accounted for 251 incidents. The different strains of viruses rose by 5 times that of 2007 and dozens of websites are attacked each month. 40 cases related to hi-tech crimes that incurred losses of VND30,000 million (10 times that of 2007).

During the conference, a discussion entitled “Information Security Strategy for Enterprises and Organisations” was also held to cover issues relating to information security policies, *information security management systems*, risk evaluation and classification, products and solutions for risk evaluation and management.

In 2009 so far, 42 websites have been attacked due to their vulnerability. Among them, there were many websites with the .gov.vn and .edu.vn domain names. Therefore, the session concentrated on two growing concerns in Vietnam: “.vn” domain name and security for wireless networks.

The main conference also showcased the latest software systems, tools, equipment and solutions for anti-virus/spam/spyware, data management and storage, web security appliances, *surveillance and identity management*. Among the leading software providers attending the exhibition were Symantec, IBM, CE Infosys, Checkpoint (Misoft), Nokia (M.Tech), Tumbleweed, PineApp, Secure Metric, Amigo and Bkav Pro.

Ngoc Khanh

<http://english.vovnews.vn/Home/Effective-IT-security-strategy-needed/20093/102858.vov>



Security World 2009 to be held in Hanoi

17:25' 02/03/2009 (GMT+7)

VietNamNet Bridge – The fourth international workshop and exhibition on security, Security World, will take place on March 24-25 at the Deawoo Hotel, Hanoi.

The event is co-organised by the General Department of Technology under the Ministry of Public Security, the Vietnam Centre for Emergency Response (VNCERT) under the Ministry of Information and Communications and the International Data Group (IDG).



With the theme “Effective security strategy in crisis”, Security World 2009 will discuss burning issues of information security in the current context of economic slowdown. The changing business environment poses bigger risks for businesses. Building an effective information security strategy at a reasonable cost is vital for all enterprises.

Security World is an annual technological forum held for IT leaders, IT experts and national IT security policy-making agencies. The event is being held to raise national information security capacity, build information security strategies for enterprises and organisations and introduce information security technology and equipment.

This year, Security World will focus on risk management, network security, anti-virus, domain name protection, digital certification, information security in finance and banking, new standards for security in the world and Vietnam.

Security World will bring about a broader view of Vietnam's national information security strategy through presentations by VNCERT, the Public Security Ministry's General Department of Technology and the Home Affairs Ministry's Government Secrecy Agency.

Further information is available at securityworld.com.vn.

VietNamNet/IDG Vietnam

<http://english.vietnamnet.vn/ITTelecom/2009/03/833663/>



“Secure your organization in an insecure era”

16:30 | 24/03/2009



CPV: The 4th Security World 2009 Conference and Showcase titled “Secure your organization in an insecure era” will be held on 24-25 March 2009 in Hanoi and co-organized by General Department of Technology - Ministry of Public Security (MoPS), Vietnam Computer Emergency Response (VNCERT) – Ministry of Information and Communications (MIC) and International Data Group (IDG Vietnam).

Featuring this theme, the event will mention the hottest issues of information security in economic downturn era. In a volatile economy, enterprises are facing higher security threats, from cyber crime attacks to theft of valuable corporate information. The vital question for organizations is how to establish an effective information security strategy which ensures business continuity within tightened budgets.

Information Security facts in Vietnam

According to MoPS (E15), numerous security vulnerabilities exist in Vietnam, nearly 60 millions computers have been infected by virus. There were 416 website hacking incidents while international hackers accounted for 251 incidents.

Mr. Nguyen Tu Quang, Director of Bkis commented that: “After two silent years, IT crimes have come back, there have been instances of attacks such as P.A Vietnam company domain theft, Techcombank website hacking, DDos attack,...Last year, the outbreak of virus was regarded as a remarkable concern in Vietnam as malicious code booms on daily basis. Apart from the proliferation of viruses, the applied technology for virus production and malware distribution has been growing rampantly”.

Bkis research released that virus strain soared 5 times higher against 2007, several tens websites have been attacked each month. 40 cases related to hi-tech crimes which incurred loss of 30 thousands million VND (10 times in comparison to damage in 2007).

Security World 2009 Conference and Showcase

This is an annual event which aims to seek solutions and technology for public security demand and national requirement in security fields such as: networking security, data protection, surveillance system, hi-tech crime prevention...



The event comes up with critical issues in National Information Security Strategy and Technology Platform for Public Security such as the nation's Information Security Strategy: laws and regulations, standards and politics, data encryption standard, cooperation of national information security authority.

Security World 2009 will be held in the context of IT budget cuts included security spending due to the pressure of an economic downturn. Hence, the event will focus on awareness improvement, practices exchange and solutions introduction aim to establish effective security strategy for IT and telecommunication system of institutes and enterprises in turmoil economy.

According to Ministry of Public Security, in the first quarter of this year, 42 websites have been attacked via security vulnerabilities. Among them, there were many websites register .gov.vn, edu.vn domain. Therefore, taking place in second day, the session will concentrate on two growing concerns in Vietnam: .VN domain name and DNS Security and Security for Wireless Network (Wifi-Wimax).

Together with the main conference, Security World 2009 also showcases the latest software systems, tools, equipment and solutions on Anti-Virus/Spam/Spyware, Data Management and Storage, Security Compliance Control, Web Security Appliances, Surveillance and Identity Management ...Vendors and exhibitors will be from noted international vendors: Symantec, IBM, CE Infosys, Checkpoint (Misoft).

http://dangcongsan.vn/cpv/Modules/News_English/News_Detail_E.aspx?CN_ID=332232&CO_ID=30293