2010

Security Information Supplied by Australian Internet Service Providers

Patryk Szewczyk
Edith Cowan University

Originally published in the Proceedings of the 8th Australian Information Security Mangement Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Security Information Supplied by Australian Internet Service Providers

Patryk Szewczyk
secau – Security Research Centre
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
p.szewczyk@ecu.edu.au

Abstract

Results from previous studies indicate that numerous Internet Service Providers within Australia either have inadequately trained staff, or refuse to provide security support to end-users. This paper examines the security information supplied by Internet Service Providers on their website. Specifically content relating to securing; a wireless network, an ADSL router, and a Microsoft Windows based workstation. A further examination looked at the accuracy, currency, and accessibility of information provided. Results indicate that the information supplied by Internet Service Providers is either inadequate or may in fact further deter the end-user from appropriately securing their computer and networking devices.

Keywords

ADSL routers, wireless networking, computer security, Internet Service Providers, end-users

INTRODUCTION

Internet Service Providers (ISPs) often ship ADSL routers preconfigured with the client's username and password thus eliminating the difficulty faced by novice computer users in accessing the Internet. It could be argued that each additional element of security may make the device comparatively less convenient to setup and utilise as a result of the protective barriers in place. Should an end-user purchase a wireless capable ADSL router, the wireless feature will be pre-enabled. However the security aspects are in most instances, disabled. Whilst paying for the service of a broadband connection, end-users are entitled to seek support from their ISP to configure their device and access the Internet. An ISP may happily provide support to successfully setup a customer's workstation and networking devices to access the Internet, however providing successful, accurate, security support may yield different outcomes.

In a recent study of verbal telephone support provided by Australian ISPs (Szewczyk & Valli, 2010) it was identified that many help desk support staff are either reluctant to provide security advise, or lack the knowledge and skill set. The study demonstrated that this resulted in false or misleading information being conveyed to the researcher. More interestingly, amongst the seven ISPs examined within the study, numerous technical support staff suggested utilising the support on their website. This is often communicated to end-users as a means to obtain security support and advice to effectively secure the end-users workstation and networking devices (Furnell, Shams, & Phippen, 2008).

There are few online avenues for an end-user to seek security information for their electronic devices. The Australian Government released two main information portals namely CyberSmart (CyberSmart, 2010) and StaySmartOnline (StaySmartOnline, 2010). Unfortunately, neither of these information portals contains beneficial information for an end-user to utilise for safeguarding their wireless network and/or ADSL router. Alternatively, an end-user may seek support from a computer retail outlet. However, in many instances, there are large fees associated with obtaining such a service which may deter an individual from utilising such a service.

It has become evident through previous research (Szewczyk & Valli, 2010) that the ISP technical support staff tends to direct the end-user towards utilising the information available from their website to secure their computers and networking devices. This paper presents an analysis of the security information provided on the websites of eleven ISPs in Australia. This paper examines the information provided for securing; a wireless network, an ADSL router, and a Microsoft Windows based workstation.

Empirical investigations conducted by Tan and Wei (2006) demonstrated that a well structured website will facilitate end-users in locating desirable information and accomplishing their goals. Hence, security information on each ISP website should be easy to locate and designed in a manner which will permit the end-user to navigate to required sections with ease. In the same manner in which an obsolete medical website may be dangerous to one's health (Roberts & Copeland, 2001) – obsolete computer security information may have disastrous effects on an individual's internet experience, or personal integrity. With the ever changing nature of security and the threats traversing the Internet, it is vital for those providing support to continually monitor and update the information they provide to end-users.

ISP SECURITY SUPPORT

For the purposes of the study eleven ISPs were selected. These were based on the predominant service providers in Australia in 2010. Table 1 details the ISPs which had their online security information analysed.

Table 7 Internet Service Providers Selected for Study

Iinet	Dodo
Westnet	Amnet
Bigpond	AAPT
Optus	Virgin Broadband
TPG	Netspace
iPrimus	

The analysis was centred on three main areas of information, specifically securing; a wireless network, an ADSL router, and a Microsoft Windows based workstation. An ISP could not reasonably be expected to provide solutions in all security areas, and for all computing and networking devices. However, it could be expected that if an ISP encourages an end-user to utilise the information found on the ISP website, that the information would at the very least be easily accessible, accurate, current, and conforming to best practices. Many ISPs sell or provide ADSL routers with wireless capability to end-users. As a result, an ISP should take responsibility and provide at least a basic after sales supportive service to secure these devices.

For the information pertaining to wireless security, there are a series of best practices home users may utilise to secure a wireless network. For example to secure a wireless connection best practice may include (Watching the Net, 2010);

- Renaming and hiding the Service Set Identifier (SSID)
- Enable Media Access Control (MAC) address filtering
- Using WPA or WPA2 encryption
- Changing the default router IP address
- Disabling the wireless feature entirely

Best practice for ADSL security may include;

- Changing the default username and password
- Updating to the latest and stable firmware
- Enabling Network Address Translation (NAT)
- Enabling the base firewall rule sets

To secure a computer according to best practice would require;

- Installing and updating sound anti-virus software
- Installing, configuring and updating firewall software
- Enabling and updating the operating system

METHODOLOGY

Each ISP website had its start-up page accessed by Internet Explorer 8. From here on the researcher manually navigated, and personally scrutinised the content of each sites one-by-one. Each ISP was awarded points for the overall content and quality of the information supplied. Three criterions were utilised to evaluate the information namely;

- Well defined definitions of key computing and security terms. These were to be presented in a manner suitable for a range of audiences with varying skill sets.
- Step-by-step tutorials designed to guide the end-user in configuring and securing various aspects of a computer and network.
- Screenshots clearly reflecting the hardware and software process that is being presented to the end-user.

An ISP could be awarded a maximum of three points for the aforementioned criteria. This criterion was independently applied to the content relating to; wireless security, ADSL router security, and computer security. The resulting outcomes are tabulated in the discussion.

Whilst the inclusion of security content is important, it is also vital that an ISP makes the information usable for an end-user with limited knowledge and skills of computing. As a result three criterions were utilised to evaluate the usability of the information namely;

- Accessibility was judged on the process required to locate and access the information. This was sought from the perspective of if a *help* or *security* section was provided on the default ISP page, or would an end-user be required to navigate through numerous pages – potentially deterring the user from the site
- The information was evaluated on its currency pertaining to areas such as whether or not the latest firewall or anti-virus product was being discussed and/or presented.
- The accuracy of information was evaluated from the perspective of if the information provided is correct, and applicable within today's standards, or would an end-user be further vulnerable by utilising those instructions.

Utilising the formulated criteria an ISP could again be awarded a maximum of three points. The qualitative aspects are presented hereafter, whilst the quantitative outcomes are presented in the discussion.

WIRELESS SECURITY

With almost every ISP in Australian bundling an ADSL router with wireless capability with their broadband plans, it would seem appropriate and responsible for these service providers to guide the end-user in effectively applying wireless security to the device. Westnet, iinet and Netspace presented comprehensive instructions on securing the device from a wireless perspective. All three providers presented screenshots of every step, with a simplified explanation as to why an end-user would want to choose Wi-Fi Protected Access (WPA) over Wired Equivalent Privacy (WEP).

Whilst Bigpond could be classified as one of Australia's largest and renowned telephone and ISP's, it appears to be lacking in encouraging end-users to apply wireless security. Bigpond provided five general pointers detailing basic security requirements. Unfortunately, an end-user would need to seek guidance and instructions from an alternative source as the website did provide adequate information apart from a mere glossary style wireless security section. Bigpond did encourage end-users to change and/or hide their SSID. However, this was only advised if the end-user suspected an unauthorised access attempts were initiated to the device. From this perspective, one could argue that the type of individual attempting to access this information to begin with would be one with little knowledge and a basic skill set in computing to begin with. Hence, such a user may not know if an unauthorised attempt to access the wireless access point was made in the first place. TPG in a similar manner provided simple definition style tips to end-users.

Virgin Broadband provided a detailed walk though guiding an end-user in how to setup and secure a wireless network. Whilst the information was specifically pertaining to their own proprietary product, the information could be readily applied to any wireless device as a result of the simple language utilised to explain the concepts and process. Virgin Broadband encouraged end-users to apply WPA and hide the SSID of their network which would in-turn create an additional layer of security for a home network.

ADSL ROUTER SECURITY

Overall few ISPs provided sufficient information for securing an ADSL router. Westnet, iinet and Netspace made convincing arguments to encourage end-users to change the default username and/or password of the device. This is vitally important in that numerous ADSL router malware specimens exploit devices which are utilising the default auethentication credentials (Bridges, 2008; Symantec, 2009). This security requirement was further enforced by providing guidance to the end-user on how to change these credentials amongst numerous currently available ADSL routers. Further aiding end-users, the three ISPs provided instructions for creating strong password. This was followed with an explanation demonstrating how a weak password may be easily cracked, resulting in unauthorised access to the ADSL router.

In the early releases of many Netcomm ADSL routers, the default firmware permitted an individual to remotely access the device omitting the needs for authentications credentials (Baume, 2009). Thus, it would seem appropriate for an ISP to provide at the very least, the guidance to inform end-users as to how to update the firmware (operating system) of the device. Unfortunately only iPrimus provided a detailed set of instructions on undertaking this task. In addition, the iPrimus walkthrough provided a detailed set of instructions for numerous, currently available models available in the Australian market. Although this may seem beneficial to an end-user it did lack a detailed explanation discussing the necessity of actually updating the firmware in the first place. As a result it could be argued that an end-user coming across this information may have a well designed set of instructions, although no actual incentive or understanding as to why they should apply this fix.

COMPUTER SECURITY

It could be assumed that an ISP would not be responsible for providing any computer security support, as they are predominantly focused on the networking side of technology. Surprisingly, computer security support was the predominant information provided amongst the eleven ISPs when compared to wireless and ADSL router security.

Bigpond, iinet, Westnet and Amnet each had a section detailing the need for computer security. In line with best practices each identified the requirements for utilising a personal firewall, an anti-virus scanner, and applying appropriate operating system controls. Westnet provided links to numerous free and commercial based security products. In addition, it provided a step-by-step screenshot representation of how to install, configure and utilise AVG, Avira and Trend Micro anti-virus software.

Bigpond, Optus, Dodo each attempt to sell an all-in-one solution for safeguarding an end-users computer. In the instance of Bigpond and Optus, the security information located on the website details numerous threats currently circulating the Internet. This is followed with scare tactics detailing statistics, and the resultant outcomes of not applying a strong security solution to a computer. Fortunately each of these websites does provide a solution in encouraging the end-user to install anti-virus and firewall software. The end-user is then prompted to purchase a complete security solution from the ISP, which claims to guarantee a secure computer, preventing any of the aforementioned threats from acting upon the vulnerable workstation.

DISCUSSION

It is evident through this paper that many ISPs do not take the need to supply information for wireless, ADSL router and computer security seriously. To more thoroughly examine the information provided by ISPs on their website, a scoring system (out of three) was developed to rank the overall information supplied. An ISP was awarded points for providing a step-by-step walkthrough, clearly defining and outlining various security terminologies and following the basic best practices for securing the wireless network, ADSL router, or the workstation utilised.

As demonstrated in Table 2 below iinet and Westnet resulted in the highest score amongst the ISPs examined. Overall, ISPs tend to focus more on providing computer security information than wireless or ADSL router information. This could potentially be a result of three of these vendors wanting to sell their own propriety computer security product to end-users. Overall, it is clear that many ISPs whilst marketing their product as superior when compared to their competitors, do not wish to support and protect the end-user in safeguarding their computer and networking device.

Table 8 Quality of Security Information on ISP Websites

	Wireless Security	ADSL Router Security	Computer Security
iinet	✔ ✔ ✔	✔ ✔	✔ ✔ ✔
Westnet	✔ ✔ ✔	✔ ✔	✔ ✔ ✔
Bigpond	✔ ✔	NA	✔
Optus	NA	NA	✔
TPG	✔	NA	✔
iPrimus	NA	✔ ✔	NA
Dodo	NA	NA	NA
Amnet	NA	NA	✔ ✔
AAPT	NA	NA	NA
Virgin Broadband	✔ ✔ ✔	✔	NA
Netspace	✔ ✔	✔ ✔	NA

Whilst it may appear important for an ISP to provide security information to end-users, it is also vital that this information be easily accessible, up-to-date and accurate in terms of the information that is presented. To test this, the research analysed the complexity with which the information was accessed upon the initial visit to the website. Each ISP was awarded a score (out of three) for each of the criteria that were listed. From an accessibility perspective, this was determined through whether an end-user could easily locate a security section on the default web page, or if it requires a search through numerous pages to find the corresponding section. Currency refers to whether the information presented was up-to-date, and discusses new and applicable security technologies. The accuracy of information relates to whether

facts were given to the end-user or, if the information would actually further endanger and compromise the user's devices having utilised the ISP guidelines.

As demonstrated by Table 3, iinet and Westnet perform best in making information easily accessible. In these instances, the end-user would only need to click on the security links to be provided with a wealth of information which is both up-to-date and providing best practice guidelines. Information is then categorised via appropriate headings and device manufactures permitting end-user to locate information in a streamlined manner.

Table 9 Accessibility, Currency and Accuracy of Security Information

	Accessibility	Currency	Accuracy
iinet	✔ ✔ ✔	✔ ✔ ✔	✔ ✔ ✔
Westnet	✔ ✔ ✔	✔ ✔ ✔	✔ ✔ ✔
Bigpond	✔	✔ ✔	✔
Optus	✔	✔ ✔	✔
TPG	✔	✔ ✔	✔ ✔
iPrimus	✔	✔	✔ ✔
Dodo	NA	NA	NA
Amnet	✔ ✔	✔	✔
AAPT	NA	NA	NA
Virgin Broadband	✔	✔	✔
Netspace	✔	✔ ✔	✔ ✔ ✔

Unfortunately many web pages such as those utilised by Bigpond, Optus, TPG, iPrimus, Virgin Broadband and Netspace attempt to sell numerous products to end-users. As a result the supportive security information is hidden away to the point that an end-user is forced to search through numerous unrelated pages to find the information required. Should an end-user wish to directly search for the information, they are often in-turn presented with alternative products, rather than the actual information pertaining to the search string. This is evident through search strings as "wireless security" which often result

Most ISPs provided current and up-to-date information. Unfortunately Virgin Broadband and iPrimus made use of examples within operating systems inclusive of Windows XP and Windows Vista and made no reference to applying the strategy to Windows 7 based products. The accuracy of the information is difficult to determine in some instances as no tests were carried out to determine if the ISP based products actually conformed to quality security products. With Bigpond, Optus and Dodo attempting to sell their own product, they will of course market the product as being the best on the market, resulting in a bias, rather than conforming to best practices.

CONCLUSION

The aim of this study was to investigate the security information provided by Australian ISPs on their website. Previous research had suggested that many ISP technical support staff will attempt to encourage the end-user to seek information on their website, rather than providing a verbal – telephone based walkthrough. This study has shown that the information provided on these websites is far from adequate from both a best practices, and accessibility perspective.

In numerous instances, the security information presented was either limited to glossary style terms, which serves no real benefit to the un-skilled end-user, or omitted entirely. With very few online information portals actively supporting the end-user in securing their computer and networking products, it is not surprising that end-users are constantly targeted through various online threats. Unlike a computer or retail outlet, the ISP has a twenty-four hour business model. Hence, there is incentive for an end-user to contact the ISP, whilst in front of their computer or ADSL to discuss any security concerns or issues that they may be facing.

In a number of instances, it appears that the ISP is utilising scare tactics to encourage the end-user to purchase their own proprietary product. Whilst no tests have been conducted on these products to determine the overall quality, there are products readily available which are both free and proven to at least provide a foundation level of security. Future

research will endeavour to examine these security products sold by various ISPs to determine if they are in line with current alternative security packages, or if they are simply exploiting human ignorance.

REFERENCES

Baume, T. (2009). Netcomm NB5 Botnet – PSYB0T 2.5L. Retrieved September 10, 2009, from http://users.adam.com.au/bogaurd/PSYB0T.pdf

Bridges, L. (2008). The changing face of malware. Network Security, 2008(1), 17-20.
CyberSmart. (2010). CyberSmart - Internet and mobile safety advice and activities. Retrieved September 13, 2010, from http://www.cybersmart.gov.au/

Furnell, S., Shams, R., & Phippen, A. (2008). Who guides the little guy? Exploring security advice and guidance from retailers and ISPs. Computer Fraud & Security(12), 6-10.

Roberts, J. M., & Copeland, K. L. (2001). Clinical websites are currently dangerous to health. International Journal of Medication Informatics, 62(3), 181-187.

StaySmartOnline. (2010). Stay Smart Online - About. Retrieved October 12, 2010, from http://www.staysmartonline.gov.au/about

Symantec. (2009). Linux.Psybot—Is Your Router Secure? Retrieved March 2, 2010, from http://www.symantec.com/connect/blogs/linuxpsybot-your-router-secure

Szewczyk, P., & Valli, C. (2010). Ignorant Experts: Computer and Network Security Support from Internet Service Providers. Paper presented at the IEEE 4th International Conference on Network and System Security, Crown Conference Centre Melbourne, Victoria.

Tan, G. W., & Wei, K. K. (2006). An empirical study of Web browsing behaviour: Towards an effective Website design. Electronic Commerce Research and Applications, 5(4), 261-271.

Watching the Net. (2010). 10 Tips To Secure A Home Wireless Network. Retrieved October 10, 2010, from http://www.watchingthenet.com/10-tips-to-secure-a-home-wireless-network.

Yet Another Symbian Vulnerability Update

Nizam Uddin Bhuiyan
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
nizamb@our.ecu.edu.au

Abstract
The more the mobile devices are approaching to advance their security, the numbers of vulnerabilities are also becoming more astonishing. The number of mobile phones including smart phones is rising vertically, and so has the amount of malware activity. This report documents the latest threats in Symbian mobile industry and analyses the consequence. In addition, it will suggest the possible solution that may help individuals to protect their device & ultimately maintain the privacy.

Keywords
Symbian, Nokia vulnerability, Nokia threats, Mobile threat, Symbian malware, Symbian virus, Cell security, Consequences and counter measure for mobile threats.

BACKGROUND

The popularity of mobile has reached to sky high regardless whether you receive a blank SMS frequently or your mobile keeps sending a SMS to strangers persistently without your knowledge. According to Goode Intelligence 2009 Mobile Security Survey, "In the last couple of years, the percentage of mobile messaging traffic (SMS/MMS/e-mail) that is defined as spam or malware has risen from approximately 2% to between 20% and 30% of total traffic" (Francis, 2010). We are always worried about computer and network related virus, threats, vulnerabilities and security issues over the years because our workstations are involved with financial, intellectual or confidential transmission. In reality, network communication has emerged with mobile communication such a way that mobile is getting more advanced than ever. For example, Android OS based Google Nexus has the CPU capacity of 1GHz (Google site, 2010). Thus, users and corporations are relying on smart phones for their daily financial or communication related transaction.

Malware developers have found a new environment – 'mobile platform' to release their malicious code since they realised that the world's business is going to be heavily dependent on compact device like smart phone, PDA, and iPad. Furthermore, their choice is smartly determined as they realise that the mobile security barrier is still immature (Panda Labs Blog, 2010). As a result, we have been encountering mobile related virus, malwares and hidden attacks. In a nutshell, mobile threats have been escalating (Brenner, 2006).

Consequently, new types of threats are being added to the current list and affecting our confidential information. Despite the fact of imminent threats of mobile environment, we rely on these devices and have to upgrade to more complex ones repeatedly. Therefore, network security industry has expended its research and development to mitigate the situation as they become conscious that mobile threat is inevitable.

INTRODUCTION

Security Researchers and Communication Managers Marcus wrote, we would notice more mobile malware attack in coming years while users are feeling comfortable to store their personal details for example, financial or identification data (Westervelt, 2007). In addition, senior news editor of *Information Security Magazine* quoted on one of his articles "Hypponen claimed that he had seen over 370 different types of malware running on Symbian based mobile because it runs on over half of the smart phone in the world" (Brenner, 2007).

According to *CIO* News (Sacco, 2008), mobile related security threats are on the rise and such threat are not limited to user operating error but also unauthorized used, phishing attack and misuse of device. Higgins, 2010 explains that a survey was conducted by *Goode Intelligence* and found that 54% of organisation plan to implement mobile antivirus solution by the end of this year.

As the mobile phone is having powerful operating system nowadays, they are capable of holding large amount of information and unsecured access to Wi-Fi. Constantin, 2009 wrote that many users misjudged mobile network threats and they were not aware that the mobile was also prone to security risk.