Cybersecurity and Online Privacy: Impact of Content Filtering and Blacklisting on Cyber Security and Online Privacy

Table of Contents

Honor Pledge:

I agree to uphold the principles of honor set forth by this community in the Marymount University mission statement and the Academic Integrity Policy and Community Conduct Code, to defend these principles against abuse or misuse, and to abide by the regulations of Marymount University.

Objective of the project

The goal of this study is to determine the influence of content filtering and blacklisting on online privacy and cybersecurity. Evaluations will be carried on secured, and unsecured computer networks with the use of these safety measures to assess how security and privacy are improved when content is filtered and known sources of malicious traffic are blacklisted. From the findings of the project, security recommendation will be made to help secure computer users in their daily activities. The study will advise users on reliable safety measures for vetting inbound and outbound traffic to ascertain no malicious content gets to the network resources.

Project point of view

In the effort to counter cyber-attacks and ensure online privacy, it is critical for the users of computers to be aware of the nature of the threats they are exposed to over these network platforms. Malicious attacks are spread using various methods such as through email messages, infected websites, and malicious advertisements among others. A considerable percentage of security breaches originate from inside the organization mainly due to the users' unawareness or careless conduct such as sharing passwords and opening anonymous e-mails and attachments (Abawajy 136). Creation of awareness of such practices is the first step in averting the threats posed to their computers as well as their privacy. Studies have revealed that the levels of cyber-attacks and spreading of infected files are on the rise putting more users and their data at significant risk. Estimates are between 10 – 20 percent of all connected computers are used to launch attacks through the internet a situation that is worsened by the fact that the owners of this computers are not aware of such malware infections (Bauer 221). Little or no information at all stimulates the rate by which the malicious attacks spread.

A user who can identify an infected website, for example, will avoid visiting such site eventually saving their computer from malware attack. If another user is exposed to such a site but is unable to detect it, they will end up getting their computers infected with a virus. The difference between the two users is that one is aware of a looming threat while the other one is unaware. Other attacks are caused by risky behavior by individuals such as sharing passwords while others are set weak ones that can be easily tampered with and eventually interfere with the privacy of such users (Whitty, Doodson and Hodges 3). Despite many being aware of the potential risks associated with compromised passwords, many people fail to underline the importance of having them protected at all times. Awareness creation of such dangers and the negative impact on personal data is essential and the first step in ensuring that people embrace security measures as far as cyber crime is concerned. The effects of the awareness information are however heavily reliant on the methods used to deliver it. Several useful methods apply to creating awareness depending on the target group. Use of print media as well as using electronic methods will serve the purpose adequately. Leaflets and posters, for instance, can be used to spread the message in an organization by highlighting the sensitive issues and the required course of action to improve on data security, other methods such as organizing seminars and use of online delivery methods will all be viable in spreading the compelling message to create more awareness.

Project plan

Table 1

Activity	**Time**	**Duration**
Project planning	Month 1	2 weeks
Resource collection	Month 1	2 weeks

Project implementation	Month 2	4 weeks
Data collection	Month 3	3 weeks
Result analysis and presentation	Month 3 - Month 4	3 weeks

Project resources

In the project, the primary resources are ICT infrastructure. I will require a set of computers, storage devices for transfer of data and a network server. The set of computers will be the workstations where users can access online content and attract traffic to the computers. Through the network server, the workstations will be connected to the internet as well as to other network resources. The presence of peripheral network resources is to create a platform where all network resources are available to observation as they interact with external and internal users. Further, I will require a network management software preferably team viewer to facilitate blacklisting of known sources of malicious content.

Project Details

Use of suitable of appropriate security applications is crucial for ensuring that all inbound and outbound data is properly vetted and verified before access is granted. The act of data verification is necessary for that it detects any malicious materials that could pose any threat to the computer as well as the user data. The increased cases of malicious attacks have prompted most users to install software that can help then in filtering their data hence improved security against any malware attacks.it is estimated that in America approximately 85 percent of the privately owned infrastructure experience regular cyber -attacks putting the data stored at significant risk (Sales 1506). The concerns about the increased cyber-attacks have led to prominent people declaring that it will become a big disaster. For instance, Richard Clarke, a former White House employee, has warned of an electronic 'pearl harbor' referring to massive online intrusion by hackers and other intruders. According to research that was conducted by Price Waterhouse Coopers across 154 countries worldwide, it was established that cyber-related attacks had increased by 48% in a span of one year between 2013 and 2014 alone (Fitzpatrick and Samuel A. Dilullo 309). Further, the research revealed that the frequency of attacks differs with the sizes of the firms. In enterprises that operate in a very competitive environment, the probability is that they will regularly update their security measure as compared to those operating in less completion. The regular update is driven by the need to keep their data safe from the competitors. Most companies that become victims of cyber intrusions suffer from loss of revenue, exposed private data and even loss of investor's trust in the company's ability to handle their data. Malicious attacks could be relayed either through the internet or using other devices such as the USB to transfer data between different machines.

Security applications can either be installed while others come with the operating systems on the computer. The Windows and Linux operating systems, for example, implement some sandbox mechanisms to avert any unauthorized changes that might be made to the system without the user's knowledge or concept; such applications ensure that the computer is protected from malicious malware attack. Secure-attention-sequence is an application that provides a secure way of preventing applications hoaxing and operating system login process. The login system is sandboxed from potential threats by using the operating system pip to suspend all running processes before it is initiated. This is a secure way of preventing any automatic attack on the system without the attention of the operator. User control access is another important mechanism that prevents the application from having escalation privilege when they are run. The UAC ensure that the computer is always under protection from any malware that could escalate once executed and compromise the state of the machine as well as the user’s data. If there is any malware that is posing a threat the computer will give a signal attracting the attention of the user hence stopping its execution. Other applications provide a graphical distinction between trusted and suspicious type. The questionable ones are labeled red while the genuine ones appear in color green. This makes it easier for the user to detect when a threat is detected and give them the opportunity to get rid of them hence increasing the security of the computer.

In the establishment of the importance of the protective applications, both machines in the study will be exposed to equal chances of the threat by having one of them equipped with the security applications while the other will run without any protection. It is obvious that by the end of the study, the count of viruses and other malware infections will be entirely different. The open one will run external applications without any alerts reducing the chance of the user to interrupt and stop the malware from running. On the other hand, the protected computer will have fewer chances of experiencing any attack as the user will always be made aware of any threat. The protected computer will also be able to filter the data going in or out scanning it and allowing only the genuine ones to run. Use of the protection applications cannot be underestimated especially in the wake of increased cyber intrusion. All Users are therefore required to have such applications to ensure that their computers are always free from any harmful material that might compromise their online security.

Network management applications provide a better and safe way of filtering and controlling the network traffic in a computer. It protects the computer from accessing anything on the internet that poses a threat to the hardware. The Internet users have in the recent past experienced painful periods with their computers frequently are trapped by different network attacks. The attacks on the computer websites and networks, efforts have been made to try and counter the effects of the computers as well as the personal data stored in emails and other internet spaces. One of the best approaches to tackle such problems is the use of data mining technique; a method that helps to classify, cluster and summarize any data coming from any network. Data mining is used by a relatively high number of individuals and institutions in their security measures against external attacks like in firewalls, intrusion detection systems as well as intrusion prevention systems. It is always easier to detect any graphical message than it is to detect a textual one. The data mining technique allows network administrators to visualize traffic patterns in graphical form. The effect is that it facilitates quick analysis and a quick reaction depending on the type of data that is detected in the traffic (Bhardwa and Singh 117). With such applications, the level of security for the computers against any intrusion is greatly enhanced and any threats detected before causing any harm. One of the computers in the study that is connected to the internet will be equipped with such software while the other will not have. Running the two devices simultaneously means that every threat that will be detected and prevented in computer A will find its way to computer B undetected. The number of threats identified with computer A will be recorded and at the end of the study, the total number of the prevented threats in A will be the equivalent of the malware that gave found its way in B. The same case applies to computer users who fail to take the necessary security measures on the assumption cyber-attacks are rare. Some of the personal data that is targeted by hackers and other intruders are access to personal email account whereby they have access to all the emails received and sent. The importance of having network management applications that filter the traffic cannot be ignored at all costs. This was my mentor concerns.

The running of such a test heavily relies on the number of visitors that access the computer or use it to access the internet. As such, to ensure there is sufficient user traffic, the tow computers will be placed in public computer labs. Here users come to use the computers for research and other personal errands. In attracting inbound traffic, the computers will have unlimited access to the internet that will encourage users to access as many online platforms as possible. Additionally, social media platforms are a major contributor of inbound traffic. Users will be encouraged to access as many social sites as possible on the machines. For certainty of malicious traffic, known ethical and unethical cyber-attacks sites will also be visited to “attract” some perpetrators of cybercrimes.

Apart from the typical data mining approach, there is another more sophisticated technique that if used can make network data filtration faster and easier. Integrated Network Traffic Visualization System (INTVS) framework, is a system that integrates various models that enhance effective visualization and tracking of any threat in the network.it is a more advanced data visualization technique that can capture network data in real time. The INTVS can also categorize and show the application layer data in the real-time domain through Grid view arrangement. Furthermore, it supports and can display campus wide area wireless network traffic on a single screen for a quick view, and at the same time detect and report the security threats by data mining techniques actually (Bhardwa and Singh 129). This is a technique that in future will revolutionize the traffic monitoring of all networks

Ethical standards in the use of technology system are an import factors as far as cyber-crime is concerned. Unethical behavior in the field of technology is becoming an important security concern for individuals and the society in general. It poses serious threats to the information system security with activities such as hacking, spoofing and software piracy being on the rise (Sutirtha and Suprateek Sarker 50). The central idea of technological innovations and inventions is to add more value to it rather than causing harm to the users (Jr., Briggs and

Derrick 11). The study, therefore, supports any efforts made by individuals to create more value for their life and others through the use of technology. The easy access to the internet has significantly contributed to the increased immoral behaviors. In most cases, however, the unethical issue in technology that involves the improper use of the internet is illegal. In most organizations, the major threat is presented by employees who use the information system facilities provided ethically. The issues of ethics do not only affect the using of technology but should cover all activities from the designing stage. Programmers should observe high ethical standards when designing a program that will be used by either an individual or an institution. Cutting corners to beat the deadline is unethical and poses serious threats to the users in case the final product of the program is not reliable (Sojer, Alexy and Kleiknecht 289).

Ethics are critical in preventing the type of criminal activities that are stimulated by the technology. An employee, for example, may decide to use the password that allows him/her to access an organization's database to log into the system and leak important details about the company to outsiders. In doing that, the employee will have gone against the ethics of his/her job and at the same time put the organization at risk. Another example is where a programmer designed a program to be used by an organization and later use the codes he/she developed the program with to have illegal access to the system. Apart from cyber crime, there are other forms of activities that are illegal that have been motivated by the development of technology. The ability of most devices to have video or audio recording application is a factor that is used by many to tap secretly into conversations of others. It not only ethically wrong to do so, but according to the law, it is illegal (Brown and Bast 744).With the anticipated future growth in the system information field, it is important to emphasize on ethical standards and draft clear guidelines to regulate the misuse of cyberspace and technological capabilities.

Risk factors

In carrying out this project, I will solely rely on software and personal input. This requires a lot of focus and a clear understanding of the subject of the study. A lapse of concentration in the project will imply deviation from the intended project outcomes. Being a security related research, the resources at use will be prone to the threats in the test. Some of the malicious cyber activity being studied may well harm the computer and personal data on the study resources. Technology age is a risk that the project will face from the onset. Though security systems are continuously improved to cover new found security threats. Malicious individuals are also coming up with new methods to carry out their activities. Use of outdated technology in the study may mean a leeway for malicious traffic. On the other hand, new technology cannot be fully reliable as it has not undergone sufficient on task tests to ensure it is completely foolproof. Organizational setting implies that the project must comply with the norms and values of the study organization. In this case, where the study is being carried on the school premises, it must not in bend the rules of the school. The organizational setting also relates to the resources available for the study. Limitation of the infrastructure, time and other relevant resources will also have an adverse impact on the outcomes of the study.

Works Cited

Abawajy, Jemal. "User preference of cyber security awareness delivery methods." *Behaviour & Information Technology* (2014): 236-247. Print.

Bauer, Michel van Eeten and Johannes M. "Emerging Threats to Internet Security: Incentives,Externalities and Policy Implications." *Journal of Contingencies and Crisis Management* (2009): 221-232. Print.

Bhardwa, Amit Kumar and Maninder Singh. "Data mining-based integrated network traffic visualization framework for threat detection." *Neural Comput & Applic* (2015): 117-130. Print.

Brown, Cynthia A. and Carol M Bast. "Professional Responsibility: Making "Smart" Ethical Decisions While Making the Most of "Smart" Technology." *Creighton Law Review* (N.d): 737-762. Print.

Fitzpatrick, William M. and Samuel A. Dilullo. "The Emerging Threat of Cyber Espionage." *Cyber Espionage and the S.P.I.E.S. Taxonomy* (2015): 307-336. Print.

Jr., Jay F. Nunmaker, et al. "The Last Research Mile: Achieving Both Rigor and Relevance in Information Systems Research." *Journal of Management Information Systems* (2015): 10-47. Print.

Sales, Nathan Alexander. "Regulating Cyber-Security." *North Western University Law Review* (2013): 1503-1567. Print.

Sojer, MANUEL, et al. "Understanding the Drivers of Unethical Programming Behavior: The Inappropriate Reuse of Internet-Accessible Code." *Journal of the Association for Information Systems* (2014): 287-325. Print.

Sutirtha, Chatterje and and Joseph S. Valacich Suprateek Sarker. "The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use." *Journal of Information Systems* (2015): 49-87. Print.

Whitty, Monica, James Doodson and Sadie Creese and Duncan Hodges. "Individual Differences in Cyber Security Behaviors:An Examination of Who Is Sharing Passwords." *CyberPsychology,Behavior and Social Ntworking* (2015): 3-7. Print.