IJERT
ISSN : 2278-0181
International Journal of Engineering Research & Technology
Publish & Find Papers @ www.ijert.org
BROWSE
OPEN ACCESS
Call for Papers

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 11, November-2018

Data Breach Risk Reduction through Perimeter Security and Smart Surfing

Adewale O Adebayo
Department of Computer Science,
School of Computing and Engineering Sciences,
Babcock University, Ilishan-Remo,
Ogun, Nigeria

***Abstract*— Data breach is probable, damaging and costly to organizations. There is a high probability that a data breach is through some form of hacking. It is, therefore, important to fortify network security and to surf the internet smartly in order to reduce the risk of a data breach, which this research is focused on addressing. Converging views in extant and current literature prescribe that every computer should have installed appropriate firewall and up-to-date antivirus, that network perimeter and network segments within the network should be fortified with appropriate firewall(s) and well configured router(s), and that important servers should be hardened and dedicated to providing only one service. The internet should be surfed with focus and anonymously where acceptable, while avoiding falling victim of scams and malwares.**

Keywords*— *Perimeter security; Internet security; Privacy; Network security; Browsing; Surfing

I. INTRODUCTION

A data breach is an incident in which sensitive, protected or confidential Personally Identifiable Information (PII) data has potentially been viewed, stolen or used by an individual unauthorized to do so. Incidents range from concerted attack by black hats with the backing of organized crime or national governments to careless disposal of used computer equipment or data storage media [1]. A large number of organizations have reported having suffered data breaches and more than forty five of US states have passed laws requiring that individuals be notified of security breaches [2]; [3], the catalyst for reporting data breaches to the affected individuals being the US California law that requires notice of security breaches implemented July 2003 [4]. No organization profits on its data breach. Strong economic reasons for organizations not to publicly report storage breach include damage to reputation, loss of current/future customers, liability from other state's laws, and possible lawsuits from shareholders/customers [5].

No matter the kind of computer network system, there is the need for some type of security to protect data and other network resources [6]; [7]; [8]. Noteworthy is the fact that external intrusion or hacking is the most prevalent and probable data breach method [9]; [10]; [5]; [11], and it is avoidable through simple or intermediate controls [11]. Securing network entry points, and surfing the Internet smartly are, therefore, important to reducing the risk of data breaches, which this research is focused on addressing. Implementation of adequate perimeter security and internet surfing prescriptions would raise the bar against successful hacking and result in fewer data breaches and a more secure computing environment.

Extensive literature review on the subject matter was performed. The relevant documents obtained were qualitatively analyzed for convergence, and relevant details were extracted, using inductive approach. The succeeding section presents effective perimeter security measures for personal, small office and home office, and for larger networks. The subsequent section discusses issues regarding surfing the Internet smartly.

II. SECURING AND FORTIFYING THE NETWORK PERIMETER

Network Perimeter is the entry point into a network or a computer system. Securing the perimeter protects the particular computer or the group of computers in the network from external attacks at the entry point, stopping attackers before entry [12], based upon clear understanding of business needs and processes related to the storage, processing, and transmission of data [8]. Perimeter security is the first line of defense against external attacks.

A network should generally have a firewall, which is any system or group of systems that implements and enforces any sort of access control policy between any pair of computers and/or networks, acting as the fortress wall for the protected. Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and un-trusted networks (beyond the organization's control), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks [8]. If the incoming network traffic does not fit the rules or policies defined in the firewall, the traffic is blocked or rejected and does not enter the internal part of the computer or network [12]. Network traffic gets from point A to point B based on computing device address and port number of specific application requesting the service. Network traffic is broken into small pieces called packets. The packet header identifies the source IP address and port as well as the destination IP address and port, which firewalls use to restrict or allow traffic. A basic sort of firewall known as packet filter may be used to deny all traffic from a certain source IP address or to block incoming traffic on certain ports. A firewall can adopt one of two basic policies to control access: whatever is not prohibited is allowed or whatever is not allowed is prohibited [13].The ideal configuration for firewall is to simply deny all incoming traffic and then create specific rules to allow

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 11, November-2018

communication from specific IP addresses or ports as the need arises. Wireless Local Area Network should disallow open access and allow only pre-authorized wireless Network Interface Cards [6].

Personal and cable or Digital Subscriber Line (DSL) router firewalls are two different types that a personal computer or another device, which might be the first port of call into a small office or home office network, should generally implement. The two are not mutually exclusive and should be used in conjunction with each other for added security [12]. When using this type of router, the default password and default IP address used for the internal network should be changed as soon as possible as they are easily available to attackers. It should be noted that cable home router firewall does not provide any protection for users who use a dial-up telephone connection to access the internet. The most commonly used, and probably the most effective, security measure for dial-up connections is known as "prearranged call-back" or simply "call-back". A personal firewall application, which is installed on each individual computer system, whether or not a router is providing protection for the network, provides security for the computer even on dial-up connection. Recent operating systems come with built-in firewall applications [14]. Most attacks directed against small companies' Point-Of-Sale (POS) systems can be prevented by changing administrative passwords on all POS systems, implementing a firewall or access control list on remote access/administration services, avoiding using POS systems to browse the web (or anything else on the Internet for that matter), and making sure that the POS is a Payment Card Industry Data Security Standard (PCI DSS) compliant application [15].

Firewall at each internet connection and between any demilitarized zone and the internet network, and router with strong access control list, are necessary for a more secure needs [8]. A deeper or more advanced form of packet filtering called "Stateful Inspection" (dynamic packet filtering) keeps track of the state of the communications above the source and destination ports and addresses. Rather than letting traffic in simply because it is on the right port, it validates that computer on the network actually asked to receive the traffic. It also evaluates the context of the communications and will reject it if it is not in the same context as the request. Stateful inspections use rules or filters or policies to check the dynamic state table to verify that the packet is part of a valid connection [16]. A newer requirement in the multilayer filtering systems is application filtering, which in addition filters packets based on the application payload in the network packets, and can prevent malicious attacks and enforce user policies. Application layer filtering includes web browsing and e-mail scanning and deep content analyses, including the ability to detect, inspect, and validate traffic using any port and protocol [17. Application gateway and/or application proxy firewall offer(s) a great level of protection. An application proxy mediates the communications between the two devices, such as a computer and server or one network and another. All messages terminate at the firewall, where they are captured, stored, logged, and examined. Some of these proxy servers will, upon successful screening of an incoming message, forward it to an appropriate application within the private network, but in most secure proxy servers, a message originating outside an organization cannot go any further than the firewall unless it passes all the inspection criteria implemented at the firewall and an independent application, running within the organization's network, selects the message from a storage area on the proxy server and consciously brings it inside the protected network [17]; [18]. Application proxy has the added benefit of hiding the client machine's true identity as the external communications will all appear to originate from the application proxy. The downside is that the application proxy uses a lot more memory and processing power and may slow down network performance. With recent boosts in processing power, and random access memory being less expensive, this issue is not as significant any longer.

The perimeter security should be fortified through host hardening by removal or disabling of unnecessary programs and ports, limiting access to data and configuration files, controlling users and privileges, maintaining host security logs and applying operating and application patches on a timely bases [19]. Inbound and outbound traffic should be limited to that which is necessary only and all other traffic specifically denied, besides eliminating direct access between the internet and the internal network [8]. Effective anti-virus software should also be installed, and regularly updated, on every host in the network. Protecting the network perimeter challenges include balancing security and usability, determining proper firewall design, providing access to resources for remote users, effective monitoring and reporting, need for enhanced packet inspection, and security standards compliance. Encryption, encoding messages before they enter the network or airwaves and decoding them at the receiving end of the transfer, should also be employed for authentication, privacy/confidentiality, integrity (hashing) and non-repudiation [6].

A. Intrusion Detection and Prevention systems

Perimeter security implemented by the use of firewalls is never hundred percent effective, and the external traffic entering the network is not the only attack vector that requires attention. Running an intrusion detection system (IDS) or intrusion prevention system (IPS) helps to detect malicious traffic that either slips past the firewall or originates from inside the network. IDS, a means of monitoring intrusion or alerting that an intrusion has occurred, can be network-based (NIDS) or host-based intrusion detection system (HIDS). A NIDS examines actual packets travelling the network in real time to look for suspicious activity. A HIDS examines log files and looks for entries that suggest suspicious activity. NIDS has the advantage of detecting attackers in real time. HIDS can detect attacks that do not travel the network, attempts to access files or change permissions, and changes to key system files. NIDs and HIDS can be used together to alert all the different types of attacks that might not be caught by just one [20]. An intrusion prevention system (IPS) is somewhat like a hybrid between an IDS and a firewall. When an IPS detects that there is suspected malicious traffic, it alters or creates firewall rules to simply block all traffic on the target port or block all incoming traffic from the source IP address or any number of custom responses configured. Sometimes the line between firewall, intrusion detection and intrusion

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 11, November-2018

prevention gets blurred as applications and devices come out that try to provide all-in-one detection and prevention.

Active intrusion response system (AIRS), using behavioral analysis of inter-network communications, is currently being offered against continuous behavioral attacks, of which distributed denial of service (DDoS) is a type. These systems employ signal processing, expert decision algorithms, statistical algorithms, and closed feedback techniques [21]. Active security devices on offer should be evaluated based on their self-adaptive mechanism, behavior analysis, closed feedback mechanism, countermeasures, real-time, and visualization capabilities. It is true today that firewalls, well configured routers and intrusion detection or prevention, including host hardening, will not protect from every possible computer attack, but with one or both of these technologies in place, exposure to risk is greatly reduced and security is increased. If information is highly desired or targeted for other reasons, understanding the motives, skills, and methods of our adversaries is important to any well-considered and well-prepared defense [11].

III. SURFING SMARTLY

Surfing the Internet (Net) smartly would reduce data breach incidents and increase productivity. This section therefore introduces the Net in a safer manner by exposing some of its potential pitfalls and how to avoid them, highlighting some of its potential benefits and how to harness them, and highlighting some of its challenges. Succeeding subsections are: Net Literature Review, Net Pitfalls, Avoiding Net Pitfalls, Internet Challenges, and Internet Dating.

A. Net Literature Review

Searching for relevant publications online is done using online databases, catalogues and search engines as tools, anytime anywhere. There are all-purpose (e.g. www.google.com, www.altavista.com), meta-search (e.g. www.metacrawler.com), and special-purpose (e.g. scholar.google.com) search engines. Keywords or search terms are used methodically to produce a list of potentially useful references [22]. Every document on the Net should be carefully evaluated. Remaining focused and taking a careful look at authorship, credibility and authenticity are necessary. Time should be provided for reading what is downloaded. Copies of anything vital, without breaking any copyrights, should be made as web pages can move or disappear without notice. Summary of what the literature is about, summary of evaluation of the literature and bibliographical information are necessary for refreshing the memory and avoiding plagiarism.

B. Avoiding Net Pitfalls

Some of the pitfalls of the Net are exposure to data theft, presence of malicious software, exposure to inappropriate content, cyber bullying, presence of cyber predators, and the ease of damaging one's reputation.

A threat is generally posed by computer technology on human privacy rights. Laws exists that govern privacy policies in specific countries, regions, or circumstances. Seven notable principles governing recommendations for protection of personal data are Notice (data subjects should be given notice when their data is being collected), Purpose (data should only be used for the purpose stated and not for any other purposes), Consent (data should not be disclosed without the data subject's consent), Security (collected data should be kept secure from any potential abuses), Disclosure (data subjects should be informed as to who is collecting their data), Access (data subjects should be allowed to access their data and make corrections to any inaccurate data), and Accountability (data subjects should have a method available to them to hold data collectors accountable for not following the above principles) [23]. Reading the privacy policy of visited websites and ensuring that they are in harmony with what is expected is mandatory. These privacy policies could be challenging to read, but efforts to make the information more presentable simplify the information to the point that it does not convey the extent to which users' data is being shared and sold (transparency paradox) [24].

Business should be transacted only at trusted websites, which provide secure connection indicated by the Uniform Resource Locator (URL) beginning with the prefix "https" where personal and credit details are requested. Further information may be found about the site's security by right-clicking on the web page, selecting properties, and then clicking on the certificate button. The URL in the browser must match the name in the certificate. Responsible and trustworthy websites hold certificates that are issued by licensed certification authorities. A list of the licensed authorities in the United States of America can be found on the State Department's website at www.secstate.wa.gov/ea/ca_lic.htm [25].

The use of long hard-to-guess passwords (mixture of letters, numbers and characters), not disclosed to friends and strangers, is essential. Malicious software inadvertent installation should be avoided by being extremely cautious when opening downloads or links from friends and strangers, by never clicking advertisements or answering unsolicited e-mails, by refraining from automatically clicking "yes" buttons, and by downloading legitimate software exclusively from trusted sites. Installation of genuine software only (system and application), up-to-date antivirus to guard against viruses, worms, Trojan and the likes, and activation of a personal firewall (which usually comes with the operating system) to guard against spyware [12] is demanded.

Installation of internet filtering software to guard against inappropriate contents**,** to block such sites even in other languages, is also necessary. Monitoring software may also be installed to record instant messaging and chat room conversation, as well as websites visited by kids. Internet filtering software are software you install on your computer to constrain internet exposure. They are fallible and must be supplemented by parental vigilance regarding children. Free internet content filters are available from the Australian government NetAlert website (www.netalert.gov.au/home.html). The main types are filters, labels and safe zones. Filters allow or disallow access to sites based on settings, labels based on site label, and safe zone allows access only to secure networks suitable to children, better pre-school [26].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 11, November-2018

Instant messaging may be blocked or banned to forestall cyber bullying, and the e-mail address known to the bully, if any, may be deleted and another created made known only to family and trusted friends. Cyber bullying should never be responded to but evidence should be kept and report should be made to the police or Internet Service Provider (ISP), e-mail provider, or website host.

User names and profiles should be kept generic and anonymous. Posting personal photos and personal information online should be avoided to elude Net predators**.** Parents should become part of children's online experience, learn about the Net, and be part of keeping the Net safe [27]. The possible consequences of posted photographs, videos, among others, that may be copied freely should be well known by all to avoid damaged reputation. Taking pictures or videos that could cause embarrassment online should be avoided completely [28]. Individuals should have a clear plan of what they want to achieve and remain focused while online.

C. Internet Challenges

Net challenges include difficulty in policing and inherent lack of control. It is difficult arresting and prosecuting a wrong doer on the Net. The law differs from country to country. Essential monitoring facilities are daunting and require large investment of money, time and effort. The skills required to investigate computer crimes quickly go out of date. Online crime is attractive because of these [29]. Besides, openness was part of internet design and responsible for its wide-spread success and acceptance; enforcing a level of control would be inhibiting to Net-based innovations.

D. Internet Dating

Online dating or Internet dating is a dating system which allows individuals, couples and groups to make contact and communicate with each other over the Internet, usually with the objective of developing a personal, romantic, or sexual relationship [30]. Online dating services generally require a prospective member to provide personal information. Most sites allow members to upload photos of them and browse the photos of others. Many sites are broad-based. Other sites are more specific, based on the type of members, interests, location, or relationship desired. The most successful niche sites pair people by race, sexual orientation or by religion [31]. Online daters may have more liberal social attitudes compared to the general population [32]. Virtual dating combines online dating with online gaming using avatars for people to interact in a virtual venue that resembles a real life dating environment. It allows users to explore compatibility, sense of humor and rapport. People who had a chance to interact with each other (by computer only) on a virtual tour of a museum subsequently had more successful face-to-face meetings than people who had viewed only profiles [33].

Internet dating problems: Many members of dating sites misrepresent themselves by telling flattering lies. Casual dating sites are often geared more towards short term (potentially sexual) relationships. Online predators find online dating sites especially attractive, because such sites give them an unending supply of new targets of opportunity for Internet fraud. Disreputable sites may harvest users' personal information and contacts for use in e-mail spam [34].

Dating sites safety tips: Personal information, such as email address, telephone or cell numbers, home or work address, should never be displayed on profile. An un-identifiable name should be use in signing up. Person met online to be met offline should be really known - person's full name, address, cell phone or home phone number and even the place of work, and verified before the meeting. It takes a long time to do, and the desire is for the person to take precedence in many circumstances. Care should be taken to report stalkers and harassers that are bugging or sending messages. It is vitally important to avoid sending nude photographs. Besides, it should be noted that photographs are unreliable as they could be deceptive [356].

IV. SUMMARY AND CONCLUSION

A personal computer with direct access to external network requires turning on its operating system built-in firewall, and installation of effective anti-virus software with real-time update. A small office or home office network requires a rightly configured cable or DSL router-based firewall and installed effective anti-virus software with real-time update on every host in the network to protect the perimeter and ensure maximum security for the computers. A network requiring excellent perimeter security demands at least an application gateway and an application proxy firewall. The perimeter security should also be fortified through host hardening. Effective anti-virus software with real-time update should also be installed on every host in the network. Inclusion of an intrusion detection and prevention security is also necessary.

Exploring the resources of the Net maximally requires wisdom in order to avoid its potential pitfalls. A definite purpose for accessing the Net each time and a constant focused attention is required. The site to visit should be clear or effective use of particular search engine(s) is (are) entailed. Everything online should be verified, even when published by supposed trusted sites. The computer or other devices through which the Net is accessed should be protected with firewall, up-to-date antivirus and filtering software to guard against malicious codes and abuse. Posting personally identifying information online should be avoided with limited exceptions. Niche online dating within reachable locality done with deserved care and caution is advisable.

Most data breaches are preventable through these means. However, clear understanding of business needs and processes related to the storage, processing, and transmission of data, and understanding of the motives, skills, and methods of attackers, and are important to any well-considered and well-prepared defense.

REFERENCES

[1] Wikipedia. (2012). Data Breach. Retrieved from http://en.wikipedia.org/wiki/Data_breach)
[2] Attrition. (2011). Entities that suffer large personal data incidents (list). Retrieved from http://attrition.org/errata/dataloss.
[3] PrivacyRights. (2011). A chronology of data breaches reported since the Choicepoint incidence (list). Privacy Rights Clearing House. Retrieved from http://www.privacyrights.org/ar/ChronDataBreaches.htm

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 11, November-2018

[4] National Conference of State Legislatures. (2012). State Security Breach Notification Laws. Retrieved from http://www.ncsl.org/default.aspx?tabid=13489
[5] Hasan, R., & Yurcik, W. (2006). A Statistical Analysis of Disclosed Storage Security Breaches. International Workshop on Storage Security and Survivability: in conjunction with 12th ACM Conference on Computer and Communications Security, October, 2006
[6] Jessup, L. & Valacich, J. (2007). *Information Systems today - Managing in the digital world*. Saddle River, New Jersey – Pearson Education
[7] Microsoft. (2000). *Networking Essentials Plus*. Redmond, Washington: Microsoft Press
[8] PCI Security Standards Council. (2010). PCI Data Security standard. Retrieved from: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf
[9] Adebayo, A. O., Omotosho, O. J., and Adekunle, Y. A. (2012). Statistical Insight into Breach Data toward Improved Countermeasures. *Journal of Information and Knowledge Management*, Vol. 2, No. 8, pp 40-51.
[10] Culnan, M J, and Williams, C C. (2009). How Ethics Can Enhance Organizational Privacy: Lessons from the ChoicePoint and TJX Data Breaches. *MIS Quarterly*, Vol. 33, Issue 4 (pp. 673-687)
[11] Verizon Risk Team. (2012). 2011 Data Breach Investigation Report. Retrieved from http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
[12] Bradley, T., & Carvey, H. (2006). *Essential Computer Security*. Rockland, MA, US: Syngress Publishing
[13] Parenty, T. (2003). *Digital Defense*. Boston: Harvard Business School Press
[14] Microsoft. (2004). Understanding Windows Firewall. Microsoft.com. Retrieved from www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx
[15] Verizon. (2012). Point-of-Sale Security Tips. Retrieved from www.verizon.com/enterprise/databreach
[16] Tyson, J. (2005). How Firewalls Work. Retrieved from www.howstuffworks.com/firewall.htm
[17] Kiernan, P. (2010). Network and Perimeter Security. Retrieved from download.microsoft.com/.../June_8_ME_Network%20and%20security.ppt
[18] Martin, R J, & Weadock, G E. (1997). *Bulletproofing Client/Server Systems*. New York, NY, US: McGraw-Hill
[19] Northcutt, S., Zeltzer, L., Winters, S., Kent, K., & Ritchey, R. W. (2005). *Inside Network Perimeter Security*, 2nd Ed. Indianapolis: SAMS
[20] Bradley, T. (2004). Host-based Intrusion Prevention. Retrieved from http://netsecurity.about.com/cs/firewallbooks/a/aa050804.htm
[21] Chesla, A. (2011). Active Perimeter Network Security. Retrieved from http://www.outpost24.com/files/024_TKK_Network_Study.pdf
[22] Oates, B J. (2009). *Researching Information Systems and Computing*. London: SAGE Publications
[23] Shimanek, A. E. (2001). "Do you Want Milk with those Cookies?: Complying with Safe Harbor Privacy Principles". *Journal of Corporation Law*. 26 (2): 455, 462–46
[24] Barocas, S. and Nissenbaum, H. (2014). "Big Data's End Run around Anonymity and Consent." in Privacy, Big Data, and the Public Good: Frameworks for Engagement (Eds. J. Lane, V. Stodden, S. Bender, and H. Nissenbaum). Cambridge: Cambridge University Press, pp. 44–75. Cambridge Core, doi.org/10.1017/CBO9781107590205
[25] Watson, J. (2001). *Buying and Selling Online*. London: Dorling Kindersley
[26] Young Media. (2011). Media Children. Retrieved from http://www.youngmedia.org.au/mediachildren
[27] Isafe. (2011). Eluding Internet Predators Tip Sheet. Retrieved from //xblock.isafe.org/docs/eluding_internet_predators_tip_sheet.pdf
[28] WebMd. (2011). Parenting – Internet Dangers. Retrieved from www.webmd.com/parenting/features/4-dangers-internet?
[29] Shostack, A & Stewart, A. (2009). *The new approach to Information Security*. Harlow, Essex: Pearson Education
[30] Wikipedia – Online Dating. (2012). Online dating Service. Retrieved from http://en.wikipedia.org/wiki/Online_dating_service
[31] Sullivan, J. C. (2008). "Let's Say You Want to Date a Hog Farmer". New York Times. Retrieved from http://www.nytimes.com/2008/04/27/fashion/27niche.html?_r=1&ref=fashion&oref=slogin
[32] Madden, M., & Lenhart, A. (2006). "Online daters tend to identify with more liberal social attitudes, compared with all Americans or all internet users." Pew Internet & American Life Project. Retrieved from http://www.pewinternet.org/Reports/2006/Online-Dating/05-Who-Is-Dating-Online/04-Online-daters-tendto-identify-with-more-liberal-social-attitudes.aspx?r=1
[33] Epstein, R. (2007). The Truth about Online Dating: Scientific American. Retrieved from http://www.scientificamerican.com/article.cfm?id=thetruth-about-online-da&page=4
[34] E-consultancy. (2011). Blogs. Retrieved from http://econsultancy.com/us/blog
[35] Free Date Club. (2011). Online Dating Safety. Retrieved from http://www.freedateclub.com/?L=cms.Free-Online-Dating-Safety