Mitigating Corporate Information Exposure on the Web

The purpose of this literature review is to examine how corporate companies can mitigate information exposure on the web. Throughout several sections, this paper will discuss internal and external variables that are involved in information exposure by discussing information used, workplace ethics and techniques individuals can adopt in-order for an act of non-observance to occur.

Most, many corporations will have a risk management system to handle business threats, one of those threats should incorporate aspects to the creation of information, if one can monitor what information is being created internally then it can be easier to prevent information exposure.

Information is multidirectional, to which is stated as being exposable internally or externally, both are accountable for information exposure on the web and can be mitigated by taking reasonable actions such as stopping BYOD policies, "The taxonomy of BYOD attacks is categorized into components and security attacks. The components are including user, network, software, physical and web", (Mahinderjit Singh, et al, 2014, Page 2). The "Heartbleed" case was a major BYOD environment attack as is targeted the SSL/ TLS protocol to which would attack username and password storage, 50 Million Android 4.1.1 devices were Vulnerable to "Heartbleed", (Mahinderjit Singh, et al, 2014, Page 5).

Data contained on the web is vastly increasing at an exponential rate, this data includes webpages, as of 2015, 4.57 Billion pages are on the internet; corporate or third-party developers will create the files needed to construct a website which will either produce a flawless site or more probable, a bug-ridden file in which people will find exploits.

This category can be both, internal and external, in which an internal variable could be involved, if an employee were to hold a grudge against the company, for example, an employee has just been fired but their credentials have not been revoked, they could potentially gather corporate information before dispersing or even release data beforehand.

Human error or ignorance is common within those who are rushed or are naïve, “One of the biggest risks to an organization’s information security is often not a weakness in the technology control environment,” rather, the action or inaction of employees, (*Information Supplement: Best Practices for Implementing a Security Awareness Program*, 2014, Page 1). Many businesses will provide a dedicated period to training new employees to reduce or eliminate indecent employee workflow; This is a vital weakness that needs to be addressed as patterns will occur and in this case, information could possibly be lost.

Many websites have been developed and or implemented poorly; after pen-testing all vulnerabilities, some may slip through. Injections are very frequent amongst hackers; the premise of a "command injection or shell injection attacks variants which causes arbitrary execution of commands supplied by a malicious web attacker", (Bhowmick, 2014, Page 4). The two most used injections are snippets of code that add custom functionality of a discrete and adverse nature, the purpose of a code injection is to exploit computer bugs in a compromised system to adapt the method of execution, to mitigate code injections on the web, developers must sanitize all data entry points and monitor for trusted and untrusted data sources.

"SQL injection attacks are initiated by manipulating the data input on a web form such that fragments of SQL instructions are passed to the Web application" (SQL Injection Attacks: Detection in a Web Application Environment, 2016, Page 3). An SQL based attack requires a web-platform or application to possess features such as none sanitised data points, if an attacker can input an SQL query, they can manipulate a database and return sensitive information with no authorisation.

A common courtesy of a company is to provide a free Wi-Fi network for either staff devices or guests, this opens to a technique called "phishing, also known as carding or brand spoofing, has many definitions; we want to be very careful how we define the term, since it is constantly evolving. Instead of a static definition, let's look at the primitive phishing methods" (James & Jevans, 2005, Page 10). The purpose of phishing is to attack an individual or company posing as an acclaimed source, the attacker could take the form of a social platform or more creditable, a bank. The concept of phishing is to perceive yourself as a trustworthy source in-order to manipulate an individual whereby exposing confidential information relating to usernames, passwords, bank details or revealing patterns in which passwords are based upon.

Although phishing is not a preferred choice of attack, it can be particularly effective as spam emails, these emails contain malicious scripts, when opened will cause email self-duplication and proceed to transmission. If an email of this type is sent to an employee and said employee opens the email, it does increase the chance of that email being forward to all their contacts, if the email is a business address, it will be forwarded to all staff members and continue until someone realises, at which point the damage may have already have happened.

There have been many cases to which discrete information has been gathered via a "hacking" technique, social engineering is defined as "the practice of obtaining confidential information by manipulation of legitimate users" (Man, 2008, Page 11). It focuses on the weaknesses and vulnerabilities of human nature. The fundamental concept is to find a pattern or approach to one’s routine or behaviour to gain the correct information to successfully plagiarise identification, this will give someone the ability to act as the victim. If a valuable employee has fallen into the trap of a social engineer and has given the required details, adversely, this will increase the chances of an unwanted information transfer. Social engineering relies on the gullibility of people to believe a trustworthy source.

To conclude this paper, the frequency at which corporations are finding alternative forms of defence is simply not on par with that of attack methods, with systems such as Metasploit ranging from legacy to modern day system with over 1600 payloads to distribute and vastly growing with frequent updates should be enough for companies to do more, invest resources into a generalised battle on cybersecurity. Resources may help; however, human error will always be inevitable. Corporations should implement more dedicated training time to their systems and workplace ethics that enforces employee regulations to be adhered to. Once corporations reduce the vulnerabilities within human nature, only then can they start to truly mitigate unlawful breaches where data is concerned.

References:

Bhowmick, S. (2014). Command Injection/Shell Injection (p. 4). Retrieved from https://www.exploit-db.com/docs/42593.pdf

Information Supplement: Best Practices for Implementing a Security Awareness Program. (2014) (1st ed., p. 1). Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

James, L., & Jevans, D. (2005). Phishing exposed (p. 10). Rockland, Mass: Syngress Pub. Retrieved from https://ebookcentral.proquest.com/lib/portsmouth-ebooks/reader.action?docID=254846

Mahinderjit Singh, M. (2014). SECURITY ATTACKS TAXONOMY ON BRING YOUR OWN DEVICES (BYOD) MODEL (p. 2, 5). Penang: University of Science, Malaysia. Retrieved from http://wireilla.com/papers/ijmnct/V4N5/4514ijmnct01.pdf

Man, I. (2008). Hacking the Human: Social Engineering Techniques and Security Countermeasures (p. 11). Aldershot: Ashgate. Retrieved from https://ebookcentral.proquest.com/lib/portsmouth-ebooks/detail.action?docID=438809

(SQL Injection Attacks: Detection in a Web Application Environment, 2016). (2016) (p. 3). Retrieved from http://www.dbnetworks.com/pdf/sql-injection-detection-web-environment.pdf