ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 7| Issue: 9| September 2021|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2021: 8.047 || ISI Value: 1.188

REDRESS CYBER SECURITY THREATS

Mr. Vikas P. Raut
Head – Department of Computer Science, Vikas College of Arts, Science & Commerce, Kannamwar Nagar – 2, Vikhroli (East), Mumbai – 400083,Maharashtra, India.

ABSTRACT
Identifying security vulnerabilities in an organisation operating with large number of web applications is not a major hurdle because techniques such as Data Flow Analysis and Taint Analysis are proficient enough to identify billions and millions of security vulnerabilities in web application's source code based on OWASP. Steep growth in Internet interconnections has expressively led growth in cyber-attack incidents many with critical consequences, one of the main concerns challenging cyber security analysts is arranging and sorting the vulnerabilities, as it is not practical to timely address risk extenuation of the web applications.
Cyber security teams always prefer to redress the threats preliminary on the basis of the perilous application that is managing the confidential data, a B2B website handling financial transactions would be the best example. According to Canadian statistics of 2019 about 54% of businesses suffered cyber-attacks crumbling their day to day operations, 36% of businesses suffered financial losses. Researching further I will first present overview of the most oppressed vulnerabilities followed by evaluations of extenuation techniques and finally new cyber – attack patterns in emerging technologies like smart phone technology, social media, and cloud computing featuring hypothetical observations on future research directions.
KEYWORDS : ***Cyber Security, Cyber – Attack, Vulnerabilities, Web Applications.***

INTRODUCTION

We, our economy, organisations and critical infrastructures have become principally dependent on computer network, internet and information technology solutions. Cyber attacks have become more potentially and disastrous as our reliance increases on information technology. Organisations can integrate web-page utilization as a secondary source of information to classify and prioritise cyber threats vulnerabilities, by incorporating the information attained from the sources such as web applications server logs a proper technique can be combined with the existing categorization scheme to formulate to redress cyber security threats.

A Symantec cyber crime report says that about 27 people become victim of cyber attack every second or more than one million attacks every day. Considering cyber attack to be the cheapest, convenient and less risky wherein the cyber criminals only require internet connection besides a computer and with unconstrained by geography and distance cyber crimes and criminals has kept growing since decades.

Web-pages with identified security weakness has high risk of cyber attacks as compared to low utilized web-pages. Combining the utilization of data with the existing categorized schemes, security analyst will be able to approach practically to contextually prioritize redressing activities on basis of usage statistics with the existing classifications given by OWASP Top 10.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 7| Issue: 9| September 2021|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2021: 8.047 || ISI Value: 1.188

IDENTIFYING THE CRITICAL PROBLEM

Image source: https://trustwave.azureedge.net/media/16717/2020-trustwave-global-security-report.pdf?rnd=132319806410000000

Organisation and business facing cyber threats more than ever before and even though the remediation process and its plan is critical, having a system for identifying cyber threats and addressing it is a crucial part of risk management for any business. Redressing cyber security threats is a structured way to identify the threats before they take hold of your system resolving issues that have already done damage, Phishing, Malwares and Ransom wares that avoid anti-virus software are the best examples of common attacks avenues.

IMPLEMENTATION OF THE TECHNIQUE

All most all source – code files, web-pages and its associated files are automatically collected by every web application, which is checked for vulnerabilities using Static Application Security Testing (S.A.S.T). Usage of automated tools for scanning the source code files generates a prominent numbers of findings with a brief explanation of the criticality, location, the type and many other details in a combined report known as Heat Maps.

Sample of Security Vulnerability Matrix
Security Findings - The below mentioned sample heat map features total number of findings using systematic scheme to redress the security threats which is needed while dealing with various web applications.

Security Findings -

	Definitive	Suspect	Information
High	3,636	1,800	2,700
Medium	54,450	36,000	5,400
Low	3,600	45,450	18,801

WILL (ML) MACHINE LEARNING ALGORITHMS HELPS IN REDRESS

The redressing practical approach should be by merging web page utilization data with active classification schemes by security analysts, this improve well timed redressing with limited resource utilization. ML models technique of scanning reports and logs of web application can be improved further to capitulate accurate results and to automate the process, but it depends on the numbers of web applications to be assessed and the size of data to be processed.

5 STEPS TO REDRESS THE SECURITY THREATS

a) Assessment of the Baseline Risk

For assessment of Baseline Risk we need to know the most vulnerable places in the information technology environment to setup a proper defence, which can be done reviewing the system process,

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 7| Issue: 9| September 2021|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2021: 8.047 || ISI Value: 1.188

assets and operations. We can commence with reviewing antivirus standards, wireless network configuration and patching process, scanning of devices connected to your network. Secondly reviewing the systems security design, firewall configuration and finally reviewing policies for administration of identified threats, disaster recovery options.

b) Creating a Monitoring System

Monitoring System has to be created in with a methodology that it gives out alerts on the potential issues, very important for organisations with large numbers of unsecured laptops, smart phones and internet enabled devices. Making a list of your IT security ecosystem pertaining of all security vendors, platforms, programs you have been operating through which we can keep a tab on the updates of the vendors on new threats, security patches which may need to be addressed. This monitoring system has to be designed to proactively warns you at times when a cyber attack takes place.

c) Redressing Identified Vulnerable Threats

Redressing the identified vulnerable threats could process by collecting your Risk Assessment data and by workflows of your Monitoring System. Proper assigning work with IT staff, vendors, and present security teams can chart known vulnerable, assign levels of risk, calculating efforts required to resolve and draft a plan to address the risk issues.

d) Training IT Staff in Redressing Threat Issues

Cyber threats begins from social engineering and phishing which means the entire responsibility goes on the IT staff for falling in the net of cyber criminals who attempt to force their way past other security measures. Hence IT staff should be trained cyber security.

e) Regular Practices

Keeping all the above process in regular practice will prove to guarantee the security and one can achieve the best redressing of cyber security threats. This practice has to be an ongoing process reviewing numerous times to keep your IT environment risk free with the needed security infrastructure.

CONCLUSION

This research focused on two portions of information system like understanding vulnerabilities in the present system and redressing of the cyber security threats. The paper discussed threats emerging from social media, cloud computing, smart phone technologies often taking advantage of their unique characteristics; it also discussed common set of cyber attacks found in the emerging technology as most of it technologies offer services through online and the most vulnerable attacks exploit the browser security through the hidden malware extensions. This paper also briefed the redressing process and methods for restricting cyber security threats.

ONLINE REFERENCES

1. *Laura Bell, M. B.-S. (2017). Agile Application Security*
2. *OWASP: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project*
3. *http://www.maawg.org*
4. *http://www.antiphishing.org*
5. *Australian Parliament the report of the inquiry into Cyber Crime, http://www.aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf.*
6. *Internet Security Threats Report. Symantec, http://www.symantec.com/threatreport*