Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 09, September-2018

Cyber Security and Compliance Management through a Single Integrated Platform

Mrinali Prakash Jagtap
MBA - ITBM
Symbiosis International University

Amit Ravindra Pagar
MBA - ITBM
Symbiosis International University

Tushar Bhimrao Meshram
MBA-ITBM
Symbiosis International University

Abstract **- Cyber Security is very important in today's information era, nowadays mostly all organizations are using information systems to do their business activities and to protect the data or information which these organizations are holding they need to be compliant with some cyber security norms.**
Today all the information security services/products implemented in any organization are stand-alone services like for Auditing, incident management, data security, Information Risk Management etc. Organizations are using different services from different vendors, so for now for any organization there is not a single service platform/framework which can provide a one-step solution for all their core information security practices. Due to this organizations have to spend a huge sum of money for individual services to meet the required information security standards in their organizations, these distributed services results in involvement more of physical/manual work, scattered processes, no clarity with all the information security related issues of the organization.
To overcome these problems this paper discusses a solution which provides a blend of Information Security as a service to provide organization with end-to-end one step platform/framework for all information security related aspects of the organization through one single framework. A single service that can target all the Information security related tasks of the organization right from risk assessment, mitigation, vulnerability assessment, threat response management, incident management, threat analytics, auditing, etc. This will help the organization to cover a broader aspect of security in a limited budget.

Keywords **-** ***Cyber Security, Compliance Management, Threat Detection, ISO 27001, GDPR, PCI DSS, Employee Awareness***

I. INTRODUCTION

Cyber security refers to the protection of internet connected devices which involves hardware, software and data from cyber attacks.
In a computing terms security includes cyber security as well as physical security both of which are used by the organizations to protect against unauthorized access to data centers as well as other computing systems. Information security is designed to maintain the confidentiality, integrity and availability of data, is a subset of cyber security.
To ensure CIA within an organization they must comply with some of the cyber security standards and for that they have do certain checks inside their organization like Information risk assessment, Threat Detection, Threat Analytics, Compliance Management, IT Auditing, Vulnerability Assessment and creating Awareness about Information Security among Employees.

The technique which this paper displays is after the research on the current scenario of the market, actually what approaches the companies are using to carryout security of information in their organization. The findings got from the research is that there is currently all the information security services/products implemented in any organization are stand-alone services like for Auditing, incident management, data security, Information Risk Management etc. Organizations are using different services from different vendors, so for now for any organization there is not a single service platform/framework which can provide a one-step solution for all their core information security practices. Due to this organizations have to spend a huge sum of money for individual services to meet the required information security standards in their organizations, these distributed services results in involvement more of physical/manual work, scattered processes, no clarity with all the information security related issues of the organization. Due to this standalone services companies have to pay for each and every services individually to avail these services, which results in high cost and due to this small and new start-up doesn't usually go for these services and always remains vulnerable to attacks.

To solve this problem this paper presents an framework and a working model for an cyber security service which is going to include almost all aspects of cyber security which is needed in an organization like Information risk assessment, Threat Detection, Threat Analytics, Compliance Management, IT Auditing, Vulnerability Assessment and creating Awareness about Information Security among Employees. The Important fact about this Project is that it is going to be an automation service which will automate all the above aspects of cyber security within an organization through one single platform/service with very less manual interaction. The goal of this project is to provide a blend of different cyber security services through one single platform and at Low cost so that even the small organizations can also be benefited from this type of service.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 09, September-2018

II. SERVICES OFFERED BY THE SYSTEM

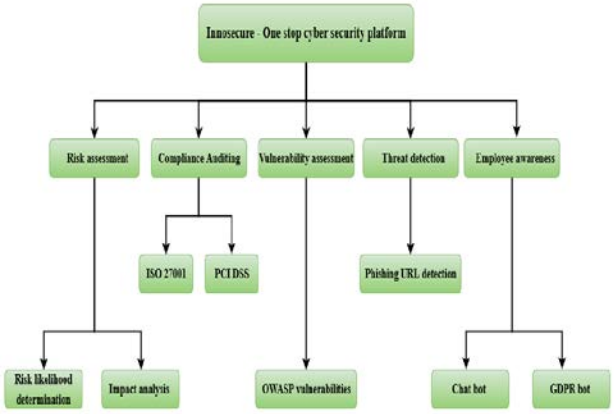


Fig. 2. Services by this system

The Services proposed by this paper is to make things automated and through one single platform and at very low cost, this makes this service different from other services currently available in the market.
The Services offered are as followed -

- Risk Assessment:

According to the probability and the severity of the risk that are identified, the system generates a risk assessment matrix and segregates the risks into three risk levels – High, Medium and Low. The risks are specified into different categories like Management, Employee, Customer, Financial and External. Solutions are provided by the system to reduce the risk level of particular risks[5].

- Compliance Auditing:

For compliance auditing the platform consists of questionnaire for ISO 27001 and PCI DSS standard. There is a provision for giving the response for each of the questions in order to automate the process. If some of the controls in the standard are not compliant, the system will suggests steps that can be taken to implement the control.

- Vulnerability Assessment:

The platform provides an open source tool for vulnerability assessment of a web application. It determines the number of occurrences of the vulnerabilities in the specific URL mentioned. Each of the vulnerabilities is segregated based on the priority as high , medium and low.

- Threat Detection:

The system provides a phishing URL detection system where it determines if a specific URL is a phishing link. We have used a machine learning algorithm – Support Vector Machine for detecting phishing URL using different features of the link. This classification algorithm determines if any specific link is a safe URL to access.

- Employee Awareness:

Employees are the first line of defense for any organization. Unfortunately, they're also the weakest link in the network security. It is an organizationsduty to improve the first part of defense by educating employees for cyber security awareness. In the platform we have provided a chat-bot for the employees which is linked to the security team of the organization. It will help them to clear their doubts regarding cyber security from the team. We have also provided a GDPR bot in the platform so the employees are aware about the latest data protection and privacy law.

III. WORKING OF THE PROPOSED SYSTEM

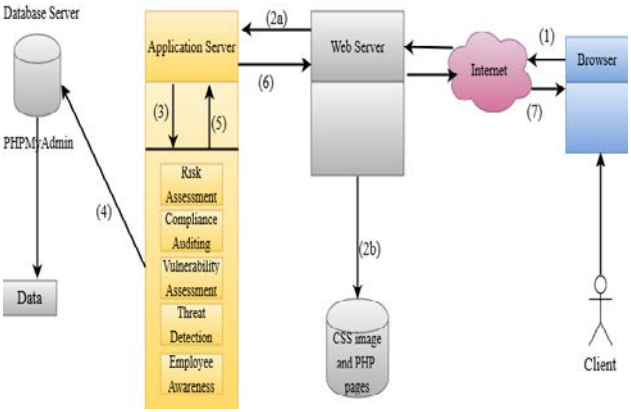


Fig. 3. Working of the proposed system

The above diagram explains seven steps process -
1) Client access the service through web browser.
2) When Client tries to access service through Web Browser it Connects to the backend web server which holds all the web pages and php to database connectivity files and applications are hosted on the Application server.
3) Application Server holds access to the Risk Assessment, Compliance Auditing, Vulnerability Assessment, Threat Detection and Employee Awareness service.
4) Application Server directs to the Database server which holds the backend data and logic files for the Application hosted on the application server
5) Once Accessing the Application data it is revert back to the Application Server.
6) Application Server throws relevant and processed data the web server.
7) Web server sends the Processed data from the Application server to the client via Web Browser.

IV. ANALYSIS OF THE SYSTEM

Each of the these Security Requirements/Problems for any organizations and how this paper resolving them through this services are described below -

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 09, September-2018

1) Automated Compliance

Compliance management is the process which ensures that a set of people are following a given set of rules. These rules mentions to the compliance standard and benchmark for compliance where as the process is what manages their compliance.

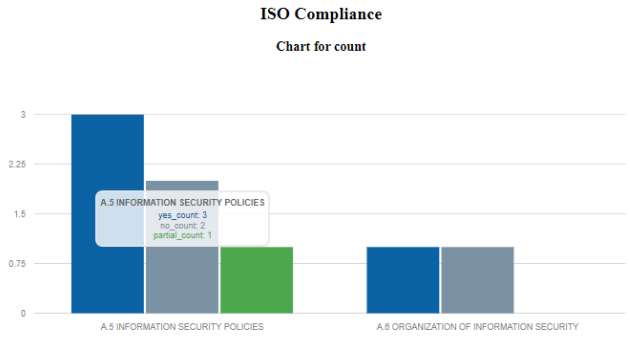
Management comliance might take different forms. It could be a mix of procedures, policies, documentation, internal auditing, security controls, third party audits and technological enforcement.

Here in this service currently ISO 27001, and PCI DSS standards are being checked for the compliance[10].

This service generates an report which takes input from the auditor's observations based on predefined sets of policies for both ISO 27001 and PCI DSS, these predefined set of policies helps the auditor to select the appropriate policies from the provided policy sets.

The below graphical representation shows what all things are compliant, non compliant and partially compliant.

View ISO Solution

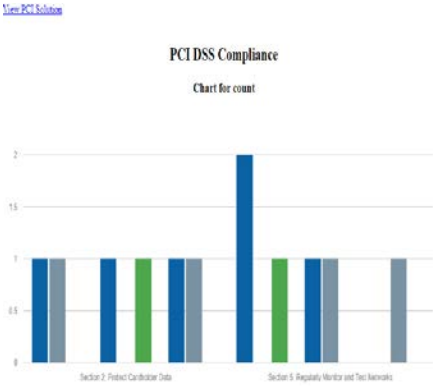


Based on the above representation, things which are not compliant a solution is provided to them so that they can come under compliance policies, below the represents the same.

Id	Question	Response	Solution
1	Do Security policies exist?	Yes	You are compliant
2	Are all policies approved by management?	Yes	You are compliant
3	Are policies properly communicated to employees?	Yes	You are compliant
4	Are security policies subject to review?	No	The organization must review the security policies time to time. The purpose of the review is to ensure the continued suitability, adequacy and effectiveness of the policies
5	Are the reviews conducted at regular intervals?	No	organizations are required to review the adopted Information Security Policy annually at a minimum
6	Are reviews conducted when circumstances change?	Partially	organizations should review their Information Security Policy on a more frequent basis particularly if significant changes occur within their organization that may have an impact on the effectiveness of the policy
7	Are responsibilities for the protection of individual assets, and for carrying out specific security processes, clearly identified and defined and communicated to the relevant parties?	Yes	You are compliant
8	Are duties and areas of responsibility separated, in order to reduce opportunities for unauthorized modification or misuse of information, or services?	No	This is the solution

Similary for the PCI DSS predefined policy set is provided, based on that auditor checks for its compliance and generate an report in graphical format and an solution set is provided to them based on number of term non compliant.

View PCI Solution



2) Threat Analytics and Detection

Threat Analytics provides a solution to help protect the organization from advanced attacks using the concept of machine leaning to predict and detect the upcoming threats[1].

Since this is an information era, huge amount of organizational data is at risk and prone to new and similar kinds of attacks. Here in this service an Threat detection mechanism is provided which uses the concept of machine learning to determine the future threats and currently Phishing Sites and keep organization ready before attack took place to tackle with it[2][3].

Here for detecting and predicting the phishing sites dataset of 41000 records are being used with 32 different characteristics of phishing sites, all these records were first tested and trained to learn the patterns for the new phishing sites[6].

Here training and testing of data is being performed using Naïve Bayes probabilistic classifier The rules for decision making are explained below:

$$\emptyset_{k|y=1} = p(x_j = k|y = 1) = \left(\frac{\sum_{i=1}^{m} \sum_{j=1}^{n_i} 1\left\{x_j^{(i)} = k \text{and} y^{(i)} = 1\right\} + 1}{\left(\sum_{i=1}^{m} 1\{y^{(i)} = 1\} n_i\right) + |V|} \right) \quad (1)$$

$$\emptyset_{k|y=1} = p(x_j = k|y = 0) = \left(\frac{\sum_{i=1}^{m} \sum_{j=1}^{n_i} 1\left\{x_j^{(i)} = k \text{ and } y^{(i)} = 0\right\} + 1}{\left(\sum_{i=1}^{m} 1\{y^{(i)} = 1\} n_i\right) + |V|} \right) \quad (2)$$

$$\emptyset_{y=1} = \frac{\sum_{i=1}^{m} 1\{y^{(i)} = 1\}}{(m)} \quad (3)$$

$\emptyset_{k|y=1}$ estimates that there is a probability that a particular feature in a phishing URL will be the k-th word in the dictionary.

For training, $\emptyset_{x|y=0}, \emptyset_{x|y=1}, \emptyset_y$ are calculated and for testing, $p(x|y = 1)\, p(y = 1)$ is compared to $p(x|y = 0)\, p(y = 0)$[11].

3) Vulnerability Assessment and penetration testing

Penetration testing (pen-testing) is a systematic way to detect security vulnerabilities in an application by evaluating the system or network with various malicious techniques. It is surely an ethical path of penetrating into a network or website, in order to bring problems to the surface with an intention to fix those[7].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 09, September-2018

Here in this service we are using an open source tool which penetrates into any websites and detects whether the site is vulnerable to any kind of attack or not[8].

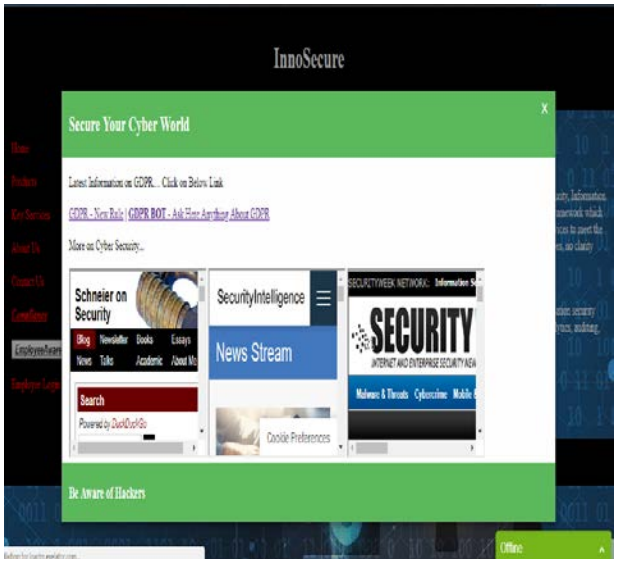
Based on the outcomes from the tool an report is being generated which shows the outcomes along with their desired proper solutions and categorizes each vulnerability based on its severity i.e. high, medium and low.

Below is the snippet of the output generated after testing "http://demo.testfire.net/".

4) Employee Awareness

Many different cyber security threats like advanced malware might only be fought with sophisticated technology. But on a daily basis, employees are the typically the greatest source of vulnerability. So that the Employees are to be that much aware that they should know their responsibility regarding organizational data[9].

Here in this service and regular update is being provided to the employees related to cyber world and latest attacks and threats, below it the snippet of this service.

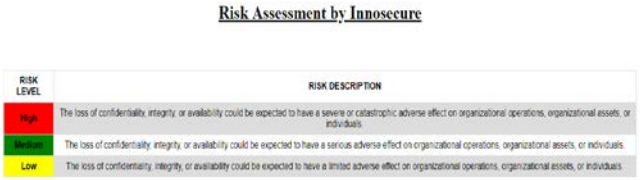


Below is the snippet of the GDPR chat bot which gives all relevant information about the latest GDPR regulation to the employees.

5) Risk Assessment

A IT risk assessment is an document that reviews the possible threats that an organization faces, natural and/or man-made. These threats are counted by the likelihood of their occurrence and then they are multiplied by their affect on the operation. This result is a value that one can use to find out if one wish to protect against the threat (mitigate or eliminate it), or ignore it[4].

Here in this service Risk is being categorized based on its level of severity i.e. High, Medium and Low.



Here in this service based on the observation of the risk assessment team particular risks are identified and using this service an Risk Assessment Matrix is being generated which shows the severity and probability of occurrence of the particular Risk. Risk which falls under Red Zone are under probability of High occurrence and so on[5].

Snippet of this Matrix is shown Below.

Here Risks are also further classified into Management Risks, Employee Risk, Customer Risks, Financial Risks and External Risk and based on their Likelihood of occurrence they are also categorized into percentage of maximum occurrence in particular category.

Snippet of it is shown Below.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 09, September-2018

Classification of risk

Sr. No.	Category	Number of Risk	Percentage
1	Management	12	37.5%
2	Employee	4	12.5%
3	Customer	7	21.875%
4	Financial	4	12.5%
5	External	5	15.625%
	Total	32	100%

V. CONCLUSION

In this paper, an approach of cyber security for any organization is proposed, where an organization can check their IT environment with an Automated tool which can assess the Risks in their environment as well as be able to do Vulnerability assessment, Detection of present as well as upcoming threats, Compliance Management and Employee Awareness in their organization and after doing all these Assessment based on the requirement this system provides them the appropriate solutions. Important thing which makes this system distinct from other system is that this is an single integrated service which includes all possible cyber security services required by any organization which makes is very cost efficient so that even small organizations can also be benefited from this service.

REFERENCES

[1] Iffat A. Gheyas and Ali E. Abdallah. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. CrossMarks 2016.

[2] Malek Ben Salem, Shlomo Hershkop and Salvatore J. Stolfo. A Survey of Insider Attack Detection Research. Springer. Insider Attack and Cyber Securitypp 69-90, 2016.

[3] AsafShabtai, RobertMoskovitchYuval and EloviciChananGlezer. Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey. Information SecurityTechnical Report. Volume 14, Issue 1, February 2009, Pages 16-29.

[4] Adrian Munteanu, Alexandru Ioan Cuza University. Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma. Managing Information in the Digital Economy: Issues & Solutions 227.

[5] L. Pan & A. Tomlinson. A Systematic Review Of Information Security Risk Assessment. International Journal Of Safety And Security Eng., Vol. 6, No. 2 (2016) 270–281.

[6] Xueni Li, Guanggang Geng, Zhiwei Yan. Phishing detection based on newly registered domains. IEEE International Conference on Big Data,2016.

[7] Konstantinos Xynos, Iain Sutherland, Huw Read. Penetration Testing and Vulnerability Assessments: A Professional Approach. International Cyber Resilience conference 2010.

[8] Prashant S. Shinde, Shrikant B. Ardhapurkar. Cyber security analysis using vulnerability assessment and penetration testing. Futuristic Trends in Research and Innovation for Social Welfare, IEEE, 06 October 2016.

[9] Ling Li, Li Xu, Hong Chen. Cyber Security Awareness and Its Impact on Employee's Behavior. Research and Practical Issues of Enterprise Information Systems. Vienna, Austria, December 13–14, 2016, Proceedings (pp.103-111)

[10] Tolga Mataracioglu. Comparison of PCI DSS and ISO/IEC 27001 Standards, ISACA Journal Volume 1, 2016.

[11] Ankit Kumar Jain and B. B. Gupta, PHISH-SAFE: URL Features-Based Phishing Detection System Using Machine Learning.