Cybersecurity Assessments

Sanjana Gadalay

Abstract*: The purpose of this study is to review the existing cybersecurity assessments and practices used by technology companies to protect their assets from potential harm and damage. Today, the software systems have thousands of vulnerabilities and, when breached, can cost the companies millions of dollars. A clear path for identifying risks, detecting threats, and responding to them is imperative. However, it is not easy to quantify cybersecurity risks as the networks and networks of networks are becoming complicated and, so most risk assessments use relevant parameters to calculate a risk score. If this score is high, it has a high impact on the critical systems. This knowledge helps hi-tech companies such as finance, banking, healthcare, defense, and supply-chain sectors to prioritize their actions and investments effectively. This study examines the risk assessment strategies and steps that companies adopt across the software development lifecycle (SDLC) to stay ahead of cybersecurity risks.

***Keywords*: Cybersecurity, Risk Assessment, Risk Scoring, Threat Modeling.**

I. INTRODUCTION

The attacks by hackers and spies in the recent past have touched almost all the world's top technology companies. Hence there is pressure from the regulatory bodies, government, media, and expectations from the customers, public, and researchers to implement cybersecurity frameworks to detect and prevent the risks early in the system. The technology companies are responsible for following the industry standards and implementing the necessary processes in their workflow to safeguard their system. They are responsible for identifying the cybersecurity risks and hazards associated with their software. They are responsible for putting appropriate mitigations in place to address data safety risks. Some companies hold terabytes of customer data, private or sensitive, such as login and passwords, bank account details, and demographics. Companies need to implement procedures into their existing risk management system to bolster cybersecurity attacks further. They need to monitor their networks systems and information systems continuously. For a product company, a strategy that encompasses the entire product lifecycle must be in place. The security measures are applied to all the phases - the design phase, development phase, integration phase, and testing phase to verify the effectiveness of their product's safety and security stipulations.

II. CYBERSECURITY STANDARDS

Some of the common standards that provide guidelines on cybersecurity are the International Organization of Standardization (ISO), International Electrotechnical Commission (IEC), North American Reliability Corporation (NERC), and National Institute of Standards and Technology (NIST) [8].

The ISO/IEC [2, 7] provides security guidelines for any digital information ISO/IEC 27000:2018, information security management system ISO/IEC 27001:2018 and Code of practice for information security controls ISO/IEC 27002:2018,

The NIST [5, 6] guides organizations to evaluate and enhance their capability to identify, protect, detect, respond, and recover from cybersecurity attacks. This framework acts as a guide for assessing and improving the cybersecurity strategy.

Fig. 1 NIST Cybersecurity Assessment Framework [6]

Revised Manuscript Received on November 20, 2020.
***** Correspondence Author
Sanjana Gadalay*, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology (MGIT), Hyderabad, India. Email: sanjana2300@gmail.com

Fig 1. shows the NIST cybersecurity framework for the functions and categories.

III. CYBERSECURITY ASSESSMENT IN THE LIFECYCLE

There is no straight path to get to a 100% cybersecurity system. It depends on the product lifecycle and what goes into each lifecycle phase.

In the Requirements phase, we establish security requirements, create quality gates/bug bars, and perform security privacy risk assessments.

In the Design phase, we establish design requirements, perform Attack Surface Analysis reduction and Threat Modeling.

In the Development phase, we use the approved tools, deprecate unsafe functions, and perform Static Analysis.

In the Vulnerability assessment phase, we perform dynamic analysis, perform Fuzz Testing, conduct an Attack Surface review.

In the Deployment phase, we create an Incident Response plan, conduct Final Security review, and certify Release and Archive.

Finally, in the Maintenance phase, Incident Response Plan is executed.

IV. CONSIDERING THREAT MODELING FOR DESIGN

Threat Modeling is a process that helps detect potential vulnerabilities and design flaws that allows unauthorized entry and gives access to attackers. The threat modeling consists of reviewing the architecture designs, data flow, and data classification in a system.

Threat Modeling happens in the Design phase. In Threat Modeling, the primary step is to establish Security Objectives for the application in review; the next step is to identify vulnerabilities, decompose the application, and identify threats at each level.

Threat Modeling is a critical step when building a new application/system or updating an existing application/system.

V. STRIDE FOR DETAILED DESIGN EVALUATION

One of the well-known Threat Modeling methods is STRIDE [12], used for the evaluation of system detail design. This is applied to cyber-only and cyber-physical systems. STRIDE is used to identify system entities, events, and the boundaries of the system.

The STRIDE exploits that are used by the attacker are

Spoofing [identity] - identifying authentication threats

Tampering [with data] - identifying threats to data integrity

Repudiation - The act of refuse authoring of something that happened, not logging events

Information disclosure - identifying data stewardship threats and data leaks

Denial of service - identifying threats to availability

Elevation of privilege - identifying authorization vulnerabilities

STRIDE is implemented by most of the companies as part of Threat Modeling and integrated within the software development lifecycle.

VI. DREAD

The DREAD [12] is another Threat Modeling method used by some companies to classify threats and in rate the threats using the below five categories.

Damage Potential - If threat exploitation occurs, how much damage is caused

Reproducibility – How easy is to reproduce the threat exploit?

Exploitability – How much efforts, skills and tools are needed to exploit the threat

Affected Users - How many users will be affected?

Discoverability -How easy to discover this threat?

DREAD risk is calculated as

(DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5

VII. COMMON VULNERABILITY SCORING SYSTEM (CVSS)

Common Vulnerability Scoring System or CVSS [10, 11] is a framework from the Forum of Incident Response and Security Teams (FIRST). It is an industry-standard supported by NIST and the U.S Food and Drug Administration (FDA.) In CVSS, each vector element has a value and computes a single score as a weighted sum of those values. The industry has widely adopted the CVSS framework. There are three groups in CVSS for scoring, as shown in Fig 3. – Base Metrics group, Temporal Metric group, and Environmental Metric group. In the Base Metric Group, vulnerability characteristics are constant with time and across user environments.

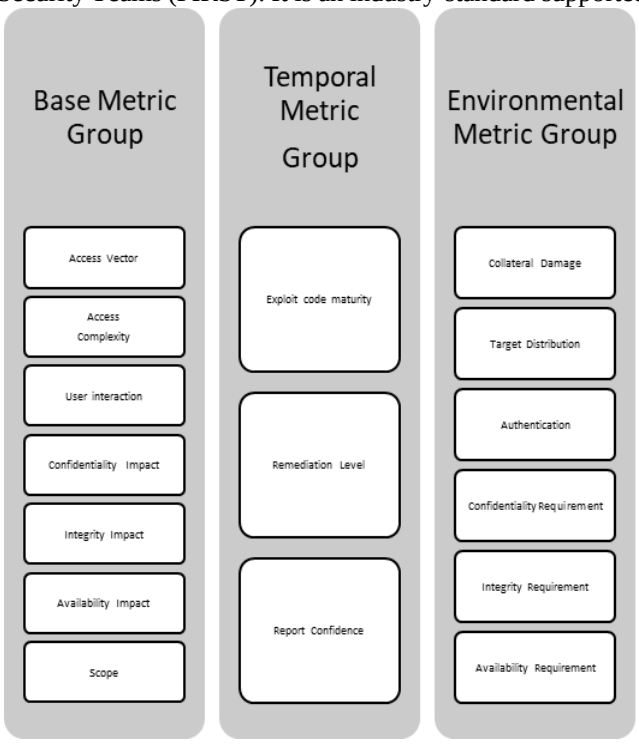

Fig. 2 The CVSS Framework

In the Temporal Metric group, the threat posed by a vulnerability may change over time. In the Environmental metric group, characteristics of exposure associates with a user's IT environment.

The CVSS Scores and Ratings are as follows -

0.0	-	None
0.1-3.9	-	Low
4.0-6.9	-	Medium
7.0-8.9	-	High
9.0-10.0	-	Critical

VIII. SOFTWARE SYSTEM ASSESSMENTS

The other cybersecurity assessments in the software innovation lifecycle are Risk Analysis, assessment of Source Code functions, assessment of Web Services or APIs, Vulnerability analysis, Static and runtime dynamic analysis, Fuzz testing, Penetration Testing, and Anti Malware Testing. The healthcare technology companies apply the standards stated by the Health Insurance Portability and Accountability Act (HIPAA) to protect patient's sensitive health information. In the finance sector, the US payment card industry (PCI) standards are used. EU regulations has recently provided a standards called the General Data Protection Regulation (GDPR) to address privacy and data control of EU citizens.

IX. COMMON ASSESSMENT TOOLS

Some standard cybersecurity assessment tools implemented by technology companies are Nmap, SQLMap, and SQLninja to identify SQL injection vulnerabilities in the databases, Nikto web scanning tool, OpenVAS Vulnerability scanning tool, Wireshark traffic and packet sniffing tool, Maltego social engineering attacks analyzer, FOCA hidden information detector, Medusa, HashCat. John The Ripper - password vulnerability detection, coWPAtty, AirCrack-NG WiFi network attack analysis.

X. CONCLUSION

This paper explored various risk assessment strategies that help identify and detect risks so companies can protect, respond, and recover from the cybersecurity risks. We looked at risk assessment frameworks such as NIST Cybersecurity Framework, CVSS scoring, Threat Modeling tools - STRIDE and DREAD. The study tells that identifying and preventing vulnerabilities in the early phases of the software development lifecycle is binding on the companies.

ACKNOWLEDGMENT

I would like to thank my family for supporting me in studying writing this paper on cybersecurity assessments.

REFERENCES

1. Dennis Hansen, "Project SAVE: Social Vulnerability & Assessment Framework", Ed. Royal Danish Defence College, 2017.
2. Alan Calder, "NIST Cybersecurity Framework: A pocket guide", Ed. IT Governance Publishing Ltd, 2018.
3. By Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, Abdul Aslam, Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats. Apress, 2015.
4. Peter Trim, Yang-Im Lee, "Cyber Security Management: A Governance, Risk and Compliance Framework". Taylor & Francis, 2016, PP 77-98.
5. Wole Akpose, "NIST Cybersecurity Framework: A practitioner's perspective" 6igma Associates, 2016.
6. National Institute of Standards and Technology (NIST) (2017a). Framework for Improving Critical Infrastructure Cybersecurity at: *https://www.nist.gov/cyberframework/draft-version-11*,*https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf*
7. ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems -- Requirements: *http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=54534*
8. NIST Special Publication 800–30R1: Guide for conducting risk assessments, NIST, pp. 95, September 2012.
9. Singhal and X. Ou, "Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs", Computer, pp. 24, 2011.
10. P. Cheng, L. Wang, S. Jajodia and A. Singhal, "Aggregating CVSS base scores for semantics-rich network security metrics", Proceedings of the IEEE Symposium on Reliable Distributed Systems, pp. 31-40, 2012.
11. "Common Vulnerability Scoring System v3.0: Specification Document", Forum of Incident Response and Security Teams (FIRST), pp. 1-21, 2015.
12. Venkatesh Jagannathan, "Threat Modeling, Architecting & Designing with Security in Mind", The OWASP Foundation: https://owasp.org/www-pdf-archive/AdvancedThreatModeling.pdf

AUTHORS PROFILE

Sanjana Gadalay is an undergrad student at the Mahatma Gandhi Institute of Technology (MGIT), Hyderabad, India. She has completed courses on Cybersecurity and Artificial Intelligence and is enthusiastic about digital transformation.