Enterprise Information Security Architectures

Madhavi Dhingra
Amity University Madhya Pradesh, Gwalior
madhavi.dhingra@gmail.com

Abstract— Security world within the enterprises are continuously changing due to the evolving attacks and threats faced by them. Cyber threats and security breaches are the biggest issue which cannot be ignored. In the recent years, many organizations have faced severe attacks due to the new developed technologies. Previously, data was stored at only one location and protection of such data is easier. Nowadays, when data is stored over the cloud, it becomes difficult to ensure the confidentiality, availability and integrity of the enterprise data and information. Thus, organizations are taking a step forward for preventing their information from leakage and considering the security architectures as solution. This paper has shown the need of Enterprise security, the existing enterprise security architectures and the upcoming trends in the area of enterprise security.

Index Terms— Enterprise Information Security; Security; Enterprise Security Architecture, Information Security, Cyber Threats, Cyber Security, Enterprise Security Threats

1 INTRODUCTION

Enterprises are struggling nowadays to achieve the balance between implementing the security controls in the enterprise while allowing the employees to increase the productivity and communicate the information easily. Enterprise security is not only about protecting the infrastructure of the enterprise, but also the sensitive data flowing among the organization. Security of enterprise is done in generic manner by applying three ways [1, 2]:

- Prevention – This involves preventing the networks from intruders by avoiding security Breaches. This is normally done by implementation of firewalls.
- Detection – This process focuses on the detection of the attacks and the breaches that are done over the network.
- Recovery – Once attack occurs, recovery is essential for preventing the information asset of the enterprise that may damage due to the attack. For this, some recovery mechanisms are being employed by the enterprises.

Till date, most of the researches and works have been done in the area of prevention and detection of the attacks.

2 Motives behind Enterprise Security

Enterprise security is getting difficult primarily due to following reasons-

A. Increasing threats- Enterprise organizations are continuously attacked by newer cyber threats with the aim of stealing the confidential information. Cyber criminals, hackers are growing in a large number. It has been reported that in recent years, malwares are worse than previous attacks. Further, crime is getting more sophisticated these days. All these factors need to be managed.

B. Technology Complexity – Security experts are dealing with threats as well as maintaining the change with effect of the new technologies like cloud computing, mobile computing, Internet of things and virtualization. These new technologies are creating gap within the system which need to be addressed.

C. Legacy security procedures and techniques: From the past, many security techniques have been used in the enterprises starting from firewalls, Intrusion Detection System/ Intrusion Prevention System (IDS/IPS), to host security software (i.e., antivirus software), and to security monitoring and compliance tools (i.e., SIEM, log management, etc.). These procedures are incapable of dealing with the multidimensional threats.

All these factors led to the design and development of specialized enterprise security techniques and enterprise security architectures.

3 Motives behind Enterprise Security

There exist multiple security standards for securing and protecting the assets of the enterprises. Some organizations use the published security standards while other implemented their own security architecture depending on their requirement. There is no single uniform standard that can be applied to all enterprises. By incorporating the recommended policies and programs, effective and consistent security architecture can be developed.

A computer-implemented method (patent) comprises the following steps for the assessment of security of data in an enterprise [3].

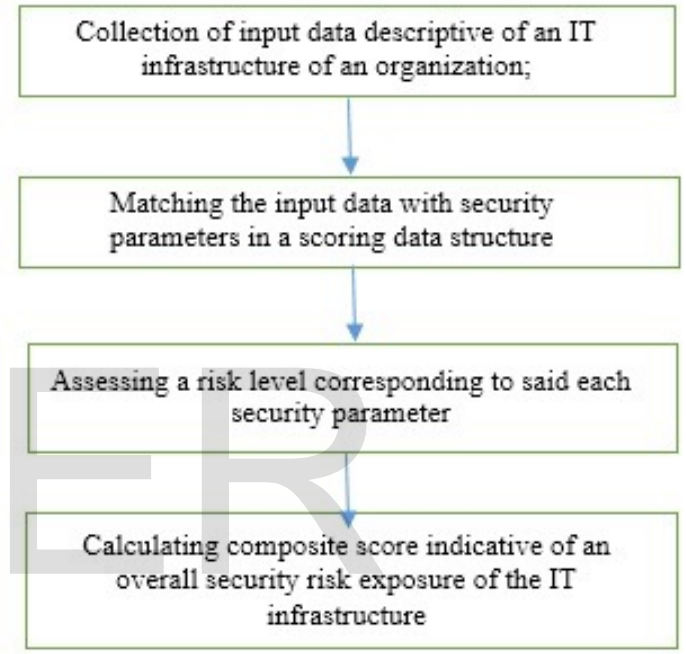

Fig. 1 Steps in a computer-implemented method [3]

Basic security architecture works on the four major things, Security Policies, Security Domains, Trust Levels and the network [4]. At every level of the enterprise, these four elements work together to build up the structured security architecture. The elements of the enterprise security architecture aid in the understanding of the enterprise security issues and isolate the vulnerabilities. The enterprise security program must address all of the infrastructure elements in order to provide true protection of information assets. Failure to address even one element of the enterprise security infrastructure leaves large holes in protection and results in little security improvement.
Every organization must be consistent with the security programs that they are planning for implementation. In many small organizations, security architecture is inherent in the enterprise security process. The problem with this is that many security processes and resources are duplicated when the security department reviews similar projects. The enterprise security architecture must ensure confidentiality, integrity, and availability throughout the enterprise and align with the corporate business objectives [5].

The objective of the security architecture is to keep away all the illegitimate users and to give timely access of resources to only authentic users. The essential property of architecture is that it must be able to bear the attack if it occurs in any condition.

Security assessment of an enterprise needs to be customized according to the security parameters of the organizations. And the investigation and analysis involved can be quite costly and time-consuming. Thus by using a common framework an organization can determine the security and privacy of the data. Enterprises follow the enterprise architecture frameworks for developing their own security architecture. A generic framework has been given which is accepted as conceptual security architecture framework [6].

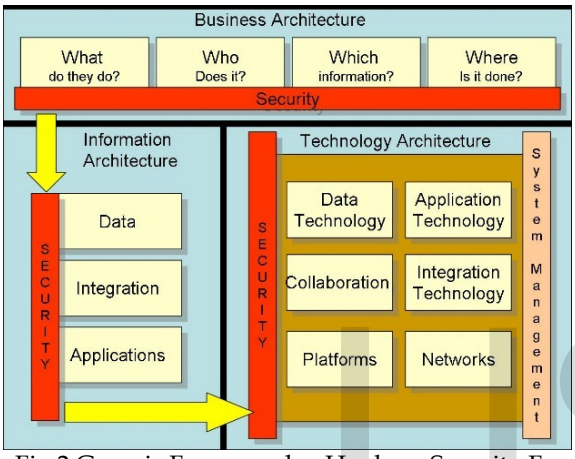

Fig.2 Generic Framework – Huxham Security Framework [7]

There are four methodologies which are mostly used at this time [7]:

1. The Zachman Framework for Enterprise Architectures—a framework and taxonomy.
2. The Open Group Architectural Framework (TOGAF)—a framework and a process.
3. The Federal Enterprise Architecture—an architecture and a methodology for creating architecture.
4. The Gartner Methodology—an architectural basis.

The most advanced enterprise-architecture methodologies like Zachman, The Open Group Architectural Framework TOGAF, The Federal Enterprise Architecture FEA, Gartner are very different in their methods. The utility of the particular architecture is decided by the security policies and requirements of the organization.

12 points of criteria are given for comparison of the four methodologies, these are shown below [8] –

	Ratings			
Criteria	Zachman	TOGAF	FEA	Gartner
Taxonomy completeness	4	2	2	1
Process completeness	1	4	2	3
Reference-model guidance	1	3	4	1
Practice guidance	1	2	2	4
Maturity model	1	1	3	2
Business focus	1	2	1	4
Governance guidance	1	2	3	3
Partitioning guidance	1	2	4	3
Prescriptive catalog	1	2	4	2
Vendor neutrality	2	4	3	1
Information availability	2	4	2	1
Time to value	1	3	1	4

Fig.3 Comparison of methodologies with ratings [8]

It has been shown that none of the enterprise-architecture methodologies is really complete. Each has its strengths and weaknesses. For many enterprises, the above methodologies do not serve the purpose. Some blended new methodology should be found for such enterprises.

4 Trends in Enterprise Security

Due to the incorporation of cloud and mobile applications, the security needed by the enterprise has been increased at a wider level. The attacks are changing day by day and so this necessitates more secure information environment. Thus these trends suggest that further improvement is needed in the security architectures of the enterprises. The key trends that are becoming popular for enterprise security are [9, 10, 11]-

- Unencrypted data

  The unencrypted data is the major problem due to which data leakage happens in the organization. Thus, application of encrypted techniques should be incorporated in the security architectures for preventing the data leakage.

- DDoS (Distributed Denial of Service Attack)

  The level of DDoS attack is getting bigger and sophisticated, so this is another concern that enterprise need to be focused on. According to recent BT research, 59 percent of companies felt that the sophistication of DDoS threats is increasing, with 40 percent of organizations saying they lacked an effective DDoS response plan.

- Managed Security Services

  Managed security services are becoming popular which can be adopted by small as well as medium scale organizations.

- Single platforms for security

  The need is to have a complete security solution for all kinds of organization. In coming years, it is expected that a single security platform will serve the purpose for all.

- Increased Customer expectations

  With the multiple kinds of threats, the customers are also demanding real time security control systems. As most of the technologies are customizing according the real-time, thus using generalize controls are no longer an efficient process.

- Data collection and processing

  Data need to be collected from the security systems as well as the enterprise databases so as to identify the correlation among the data. The collected data need to be analyzed for threat detection. It is also necessary to identify important data and sensitive data which can be kept private or public. An enterprise needs a highly adaptive cybersecurity infrastructure that is capable of quickly adding and correlating new data in combination with existing information.

- Malware analytics

  Malware analysis had been done by several years but they are sometimes ineffective against specific attacks. Enterprises need static and dynamic malware analysis tools that are able to open and execute files to search for malicious behavior. In addition to the malware detection, their behavior can also be determined before exploit and after exploit.

- Intelligent algorithms

  Security analytics tools must offer features like machine learning algorithms for better anomaly detection. Superior security analytics tools will provide nested algorithms that sequence multiple behavioral anomalies together before issuing an alert.

4. Conclusion

Enterprises are continuously developing and testing newer security policies and security architectures for protecting their data. Many organizations have developed their own security architecture. Still, the enterprises are dealing with the newer threats and are modifying their security policies day by day. This poses the need of the holistic security framework which can dynamically address the protection of data by considering all kinds of enterprise security issues including real-time attacks.

References

1. Cyber Security Research and Development Agenda, January 2003, The Institute for Information Infrastructure Protection, 2003, Cyber_Security_RD_Agenda.pdf
2. Zachman, J.: 'A framework for information systems architecture', IBM SYSTEMS JOURNAL, 1987.
3. Mark D. McGovern, Patent for Techniques for Information Security Assessment, Publication number US20090024663 A1, Publication type: Application, 2008
4. Winter, R., and Fischer, R.: 'Essential Layers, Artifacts, and Dependencies of Enterprise Architecture', Journal of Enterprise Architecture–May, 2007, pp. 1
5. Chung, L., Subramanian, N. 2007. Bridging the gap be-tween enterprise architectures and software architectures. Science of Computer Programming 66 (2007), 1-3.
6. Giachetti, R. 2012. A Flexible Approach to Realize an Enterprise Architecture. Procedia Computer Science 8 (Aug. 2012), 147-152.
7. Enterprise Security Architecture, Huxham Security Framework, wikepedia
8. Roger Sessions, A Comparison of the Top Four Enterprise-Architecture Methodologies, ObjectWatch, Inc.May 2007
9. Lyovina, A.I., Dubgorn A.S. 2014. Approach to information requirements identification of procurement process of custom production. In Recent Advances in Mathematical Methods in Applied Sciences. Proceedings of the 2014 International Conference on Mathematical Models and Methods in Applied Sciences (MMAS '14). Saint Petersburg, 2014, 401-411.
10. Problems of Data Protection in Industrial Corporations Enterprise Architecture, V.V. Glukhov, Proceedings of the 8th International Conference on Security of Information and Networks, 2015, Pages 34-37
11. Raytheon Is Addressing the Transformation in Enterprise Security, Jon Oltsik, Senior Principal Analyst, Enterprise Strategy Group April 2015