Layered Defense in Depth Model for IT Organizations

Azra Shamim, Bushra Fayyaz, and Vimala Balakrishnan

Abstract — Security methodologies are constantly changing and improving hence becoming a challenge for IT organization to keep their posture up-to-date and effective. It may be productive to examine different security postures to create and improve organization’s information security architecture. This paper discusses about defense in depth model and strategy to implement it effectively. Also fructification of each layer of model presents vast variety of implementation alternatives and adoptability according to the design and architecture of organization. Tactically, security is incomplete without proper assessment of assets, risks associated with them and policies to control these risks; the outermost layer of the model covers all these aspects. Well defined policies and procedures aid in designing best security practices for any organization. Security issues do not solve magically but administrators have to evaluate different methodologies to consider as best practice for their organization.


I. INTRODUCTION

In the modern IT environment, information and its associated technologies are exposed to wide range of security risks, including data leakage, disruption and denial of services resulting in negative impact on business continuity. To address these risks, a comprehensive information security strategy must be implemented that should support the organization’s functional and strategic plans with continual improvements to achieve higher level of security [1]. Traditionally a security baseline is defined by the organization which is enhanced as the number of security incidents increases. Different types of information security countermeasures such as virtual private networks (VPNs), Zoning, unified threat management (UTM), antivirus, patch management and encryption of data deployed by more than 60% of organizations [2]. However reports shows that organizations are facing increased number of targeted attacks originated internally as well as externally [3]. Hence, a single strategy to defense information and its associated components may not be sufficient [4]; this paper will discuss a defense in depth model with multiple protective layers.

Azra Shamim is with FSKTM, University of Malaya, Kuala Lumpur, Malaysia. (e-mail: azra.majed864@yahoo.com).
Ms Bushra Fayyaz, was with Comsats Institute of Information Technology, Islamabad, Pakistan. She is now working in Public Sector of Pakistan. (e-mail: bushra.fayyaz@gmail.com).
Vimala Balakrishnan is with FSKTM, University of Malaya, Kuala Lumpur, Malaysia. (e-mail: vimala.balakrishnan@um.edu.my).

II. DEFENSE IN DEPTH

Concept of defense in depth is adopted from military defense where different obstacles are deployed to eventually expend the resources of attacker [5]. In information security terms, administrator or organization deploy layers of defensive measures to minimize risk of unauthorized access or information attacks [6]. Overlapped layers cover shortcomings of one layer by other [7]. A well-defined and well implemented defense in depth strategy prevents a wide variety of attacks and also generates real-time intrusion alarms to the administrators [8] [9].

Defense in depth is also an effective method of mitigation and prevention of automatic attacks that an organization faces from public internet [8]. In this type of attack, attacker attempts to exploit an information system or asset in real time environment with different methods which are extremely difficult to prevent, the defense in depth architecture may provide differential protection [8]. Security measures such as Demilitarized Zones (DMZ), firewall, Intrusion detection System (IDS), Malware Protection and virtual private networks (VPNs) provide defense in depth strategy that deflect information security attacks aim to gain unauthorized access to an organization assets from the internet or public network [10]. Each of these devices acts as obstacle to the attacker [5]. Defense in depth is a verified method by testers to protect organizations’ information and its associated technologies from attackers and intruders [11]. This methodology is so flexible that it can easily adopt protection mechanisms against new emerging threats. In an ideally implemented environment security incidents or alarms are least expected by the administrators. This accomplished by highly educated, motivated and experienced administrators with organization’s higher management commitment [6].

Each layer in defense in depth architecture has heterogeneous implementation of security controls which results in administration overhead. This may lead to improper implementation and security holes for attackers. Improper deployment weaken the system, and lack of education experience leads to the difficulty in maintaining the true spirit of defense. Hence, the entire methodology is heavily depended on motivation, skill level, education, experience and determination by the administrators [12].

Despite, very well implementation of defense in depth strategy, it has inherited concedes such as: (1) attack can occur if enough time is given to the attacker to evade security controls or obstacles [13]. (2) It produces lot of overhead
which should be managed properly. Defense in depth base on layered architecture, every layer has its own implementation and management such as in network layer every OSI layer must be considered and secured; hence produces overhead for administrators [14], [15].

III. ELEMENTS OF DEFENSE IN DEPTH

A. Security Policies and Procedures

In first layer of defense organization must setup benchmarks, standards, policy and in some scenarios the legal regulations, and the best practices as baseline standard. Later these become de facto standard for any organization [16] also shown in Fig 1. Internationally different standards are recognized for security information such as International organization for standardization (ISO) [17], Payment Card Industry (PCI) Data Security Standard (DSS) [18], Control Objectives for Information and related Technology (COBIT) [19] [20] and many more. Every standard or regulation has a general implementation cycle which is shown in Fig 2

B. Physical Security

It not only concerned with locking the doors and sitting of guard but also include security of server room, laptop and desktop protection, and human factors [21] [22] [25].

C. Perimeter and Network Security

Fructification of network is core element in securing IT organization as shown in Fig 3 between major network segments. It starts with covering architecture against known and obvious network attacks [7]. The perimeter of network traffic must be filtered by stat-full inspection of firewalls, intrusion detection mechanisms, malware identification and blocking technologies, filtering of impending dangerous contents [23][24]. To defense network perimeter it is important to understand what a network might face in terms of attacks and threats. When properly configured this layer protect information assets by permitting only those activities which are required to continue business operations [26] [28].

D. Monitoring and logging of Events

Security architecture remains incomplete without proper monitoring and logging system. Network and Security operations must be continuously monitored for sign of any possible intrusion. Effective alerts and alarms can only be generated with proper implementation of monitoring of security controls instead of just parsing logs from one device to other [27]. Even complete deployment of monitoring system, administrators must review critical logs on daily basis to detect advanced intrusion or threats to system [29].

E. Host Security

Host security is important as fructification of network in security architecture. Antivirus, anti-malware, host intrusion detection and prevention mechanism, host based firewalls and operating system hardening must be implemented [30] as shown in Fig 4.

F. Session Security

It provides restrictions over a user within a unique session and it is critical in web security. Cryptographically strong, appropriate key and session identifiers are the best controls used to implement session security [31]. A complete guideline in this regard is available on OWSAP [32].

G. Application Security

Security of users, information regarding credit cards, restriction on rights, vulnerability analysis, input validation, backup and restoration, passwords and access control lists (ACLs) are the controls that supports implementation of security of application. [33][34][36]

H. Data Security and Data Leakage Prevention

Industry supported encryption such as Triple Data Encryption Standard (3DES) must be implemented to protect private data of organization and user including credit card information [33] [35].
IV. FEATURES OF DEFENSE IN DEPTH MODEL

Fig 5 shows common defense in depth model for IT organization, it covers all the elements discussed in previous section. Effectiveness of this model is restricted to education level, motivation and experience of the administrators. If it effectively implemented following are the features of defense architecture.

A. Diversification

Each layer of defense in depth model possesses variety of vendors, techniques and mechanisms. To strengthen even more, diverse infrastructure components must be deployed because of single vendor possess single attack vector [5-12] but it create lot of administrative overhead. Careful testing and proof of concept study provide maximum benefits to organization. Also place importance in ensuring that data travels through diverse medium as well as vendors to minimize one bottleneck [6].

B. Proven.

This model is tried and proven against automated and other attacks with intrusion of active attackers. In a fine tuned environment administrator least expect a security alarm or signal. [5],[9]

C. Scalable and adoptable

This layered approach is so flexible that it can easy adapt to new threats by layering in new security controls, also this model can be applied to small to large and from ordinary to military or government level organizations [6].

D. Isolation of assets

Perform risk analysis and as a treatment measure, isolate your critical assets and harden them to make sure that attacker to overcome great obstacles. Addition of more than one authentication mechanism prevents a successful attack [15].

V. CONCLUSION

Various methods of information security and defensing the architecture are in place in different organizations but defense in depth model presents most comprehensive framework for security purpose. Due to its adoptability and scalability in nature it easily provide defense against new emerging threats by utilizing new mechanisms as they become available. Haphazardly purchasing, setting up, un-educated administrators are the major pitfalls of this methodology. Human asset constraint should be kept in mind while making design of information defense strategy. Where-ever possible administrator should choose team members who are motivated, educated and experienced. Team members must be enough motivated that they should be interesting in learning and exploring new eras of information security. Well rounded security professionals with international certifications having on job training and highly motivated would be beneficent in effectively implementing defense in depth methodology.

REFERENCES


[18] https://www.pcisecuritystandards.org


[36] IT Showcase white paper, published in January 2003, detailing Microsoft IT’s Application Security practices