ISAUnited
International Security Architects

Structured Layered Defenses-RP-208

Recommended Principle

Version 1-01.2024

Forward

This guiding principle for integrating “Structured Layered Defenses aka Defense in Depth” into security architecture design. It refrains from prescribing detailed practices or instructions for every specific situation due to the intricate nature of industry and organizational technical architecture designs, encompassing infrastructure, complex networks, and associated components and systems.

Shall: As used in a standard, “shall” denotes a minimum requirement in order to conform to the standard.

Should: As used in a standard, “should” denotes a recommendation or that which is advised but not required in order to conform to the standard.

This guide should be used in conjunction with the practices described in the following ISAUnited standards and publications, when appropriate (use the latest revisions):

1. Security Design Operations Model
2. Defensible Architecture Design Methodology

Contents

Structured Layered Defenses-RP-208

Recommended Principle

Version 1-01.2024

Description

Prioritizing the imperative to ‘Structured Layered Defenses aka Defense in Depth’, this approach centers on identifying segments within an organization's architecture, particularly its infrastructure, and network. Due to potential Internet security risks occurring at various levels, you need to set up security measures that provide multiple layers of defense against these risks.

The intent of Defense in Depth is to implement multiple and independent levels of protection (armored lines) to reduce the risk of an accidental consequence such that, if one line fails, the next will come into play in delivering the security measures necessary.

Scope

Although the phrase 'Defense in Depth' is generally used as broad terminology, ISAUnited has deemed the scoped principle should follow a more focused element of 'Structured Layered Defenses'. This scopes the defenses as more strategized and planned rather than adding many layers that are not efficient, effective, and or costly to an organization.

By leveraging a proactive and strategic approach, the goal is to implement targeted security measures and risk mitigation strategies to strengthen the overall resilience of the organizational architecture which encompasses infrastructure, networks, and associated components and systems. This recommended principle (RP) establishes the base requirements of architecture security for organizations that design, operate, implement, and support architecture for use in on-premises, cloud, and or hybrid. This RP provides security practitioners with an enhanced framework to reveal and manage risk, promote a learning environment, and continually improve architecture security and integrity by using this principle. At the foundation of this RP is the practitioners' existing architecture security posture. The elements herein comprise what should be done, not how to do it. The document does not explicitly address individual personnel duties and departmental duties, but the elements herein can be applied to those aspects of an employee or operation. This principle emphasizes the critical reasons why security architects shall have an in-depth knowledge of these principle elements.

Terms, Definitions, and Abbreviations

Architecture - Technical architecture refers to the structured framework that defines the design, organization, and integration of various technological elements within an IT system or enterprise. It encompasses hardware, software, networks, databases, and other components to create a cohesive and efficient structure that supports the organization's information technology strategy. Technical architecture provides a blueprint for the implementation, maintenance, and evolution of IT systems, ensuring alignment with business goals and optimal functionality.

Infrastructure - encompasses the foundational components, facilities, and systems necessary for the operation and functionality of an organization's information technology environment. This includes hardware, such as servers, data centers, networking equipment, and storage devices, as well as the associated software, middleware, and other supporting elements. Technical infrastructure provides the underlying framework for the deployment, management, and delivery of IT services, ensuring the reliability, scalability, and performance of an organization's technological capabilities.

Network - A technical network refers to the interconnected system of devices, communication pathways, and protocols that facilitate the exchange of data and information within a computer or telecommunications environment. It encompasses the hardware components like routers, switches, and cables, as well as the software protocols and configurations that enable seamless communication between computers and other devices. Technical networks are designed to support various functionalities such as data transmission, resource sharing, and access to services, forming the backbone of modern information technology infrastructures.

Components - any part of a system that, by itself, provides all or a portion of the total functionality required of a system. A component is recursively defined to be an individual unit, not useful to further subdivide, or a collection of components up to and including the entire system. A component may be software, hardware, etc.

Systems - a system is made up of one or more components, which may be linked (interact through the same processor) and or tightly coupled.

Defense In Depth - Defense in depth in networking is a security strategy that involves implementing multiple layers of security measures and controls to protect a network from various types of threats and attacks.

Network Segmentation - Network segmentation is a security practice that involves dividing a computer network into smaller, isolated segments or subnetworks to enhance security and control access.

Security Culture

A favorable security culture is crucial for the security performance of the organization, regardless of its size or complexity. Security culture encompasses the shared attitudes, values, norms, and beliefs among employees and contractor personnel in the security department concerning risk and safety. In a positive security culture, collaboration among staff members is fostered, positive attitudes toward compliance are encouraged, a sense of responsibility for public safety and each other's well-being is instilled, and there is a fundamental belief in non-punitive reporting.

Given the numerous and intricate security activities within the organization, it is imperative to systematically manage security using an agreed framework and cultivate a positive security culture. While a positive security culture can exist independently, an effective SMS cannot thrive without it. Hence, security operators should actively strive to enhance and evaluate their security culture.

Sustaining a positive security culture demands ongoing diligence across the security department to address issues such as complacency, fear of reprisal, overconfidence, and normalization of deviance. Indicators of a positive security culture within the organization are provided below.

The organization:

- embraces security (personnel, public, and asset) as a core value,
- ensures everyone understands the organization's security mission, vision, and goals,
- fosters systematic consideration of risk, including what can go wrong,
- inspires, enables, and nurtures change, when necessary,
- allocates adequate resources to ensure individuals can accomplish their RP recommending the principle responsibilities,
- encourages employee engagement and ownership,
- fosters mutual trust at all levels, with open and honest communication,
- promotes a questioning and learning environment,
- reinforces positive behaviors and why they are important,
- encourages two-way conversations about learnings and commits to applying them throughout the organization, and
- encourages non-punitive reporting and ensures timely response to reported issues.

Adopting and implementing this recommended principle will strengthen the security culture of an organization. Leaders, managers, and employees acting to make safety performance and risk reduction decisions over time will improve architecture security as a value, thereby strengthening the security culture of an organization. With this RP, practitioners are provided an enhanced framework to manage and reduce risk and enable continual improvement in architecture security posture. The individual elements, when executed as deliberate, routine, and intentional processes result in improved communication and coordination, which yield a cohesive system and a stronger security culture.

Principle Elements

Network Segmentation:

- Divide the network into isolated segments to contain potential breaches and limit lateral movement within the network.

Lines of Defense:

- The 1st and 2nd lines of defense are necessary for the Defense in Depth concept to create a multi-layered approach that not only prevents initial attacks but also detects, responds to, and mitigates potential threats that manage to breach the first line.
    - 1st line of Defense (1LOD):
        - **Role:** The 1st line of defense is the initial layer that aims to prevent unauthorized access and protect the system or organization from external threats.
        - **Necessity:** This layer acts as a frontline deterrent, actively blocking or repelling potential threats before they can breach the security perimeter. It includes measures like firewalls, intrusion detection systems, and access controls.
        - **Importance:** By preventing threats at the first line, organizations can reduce the likelihood of successful attacks, minimizing the surface area for potential vulnerabilities.
    - 2nd line of Defense (2LOD):
        - **Role:** The 2nd line of defense acts as a backup layer, providing additional protection and containment if the 1st line is breached.
        - **Necessity:** Even with a strong 1st line, it's crucial to have a secondary layer that can detect and respond to threats that may have evaded the initial defenses. This layer includes security monitoring, incident response, and more advanced threat detection tools.
        - **Importance:** In the event of a breach, the 2nd line of defense helps identify and mitigate the impact quickly, containing the threat and preventing it from spreading further into the network or organization.

Control Plane Protection (Harden Network Infrastructure)

- Network and cloud providers implement Defense in Depth to protect the control plane of their network infrastructure. The control plane is the part of the network infrastructure that facilitates communication between network devices and network services. This layered approach uses Defense in Depth security features, such as firewalls, intrusion detection and prevention systems (IDS/IPS), anti-malware software, secure configuration guidelines, access control lists (ACLs), packet filtering, bandwidth management tools, and global threat intelligence feeds.

Data Plane Protection (Harden Data)

- Network and cloud providers implement Defense in Depth to protect the data plane of their network infrastructure. The data plane is the part of the network infrastructure that facilitates communication between network devices and network services. Cloud services typically include multiple layers (data planes) with different protocols to meet the needs of different clients better and prevent sophisticated attacks.

Endpoint Protection (Harden Stored Data)

- Network and cloud providers implement Defense in Depth to protect the endpoints devices such as laptops, desktops, tablets, and smartphones. The data on these devices is protected with encryption, secure authentication, safe application listing, application control, and run-time defenses such as application behavior monitoring (ABM), vulnerability scanning, and intrusion detection systems.

Remote Access Protection (Harden Domain)

- Network and cloud providers implement Defense in Depth to protect remote access users by implementing authentication, authorization, and encryption measures.

Data Classification Defense (Harden Data in Motion)

- Network and cloud providers implement Defense in Depth to protect data in motion by implementing detection and prevention technologies such as firewalls, network intrusion scanning, IPS systems, anti-malware systems, data loss prevention tools, secure devices, and protocols.

Responsibilities

Practitioner - The security practitioner shall establish and maintain the recommended principle and build a shared understanding of security culture. The security practitioner shall articulate expectations, including publishing a commitment to security, security responsibilities of personnel at all levels, policies, goals, and objectives. The security practitioner shall improve upon the recommended principle and measure its effectiveness and maturity in accordance with the requirements of this guidance document.

Management - Management shall actively promote, collaborate, communicate, sponsor, and provide support for this recommended principle.

General user - Users shall utilize and integrate this recommended principle into their operations and practices.

RACI - Responsibilities, accountabilities, and authorities in developing, implementing, and continuously improving the security shall be defined, documented, and communicated throughout the architecture practitioner's organization. Accountability for resource allocation shall be assigned to (an) management with appropriate authority.

Competence, Awareness, and Training

The security practitioner shall ensure that personnel whose responsibilities fall within the scope of the RP recommended principle have an appropriate level of competence in terms of education, training, knowledge, and experience. Where external resources, including contractors, are used to support the RP recommended principle, the security practitioner shall ensure that operating personnel have the requisite competence, skills, and experience.

The security practitioner shall define the need for and provide training to enable the development and implementation of the RP elements. Training shall include refresher training and raising awareness of where executing the safety assurance and continuous improvement sub-elements reveal opportunities to improve processes and procedures. Records of training shall be maintained.

The security practitioner shall establish a training schedule to ensure that personnel and contractors who have accountabilities, responsibilities, and authorities in executing the requirements of the RP are updated and aware of:

1. applicable elements of the RP recommended principle that affect their job requirements;
2. newly emerging or changing risks, problems in the execution of the RP, and opportunities to improve processes and procedures; and
3. potential consequences of failure to follow processes or procedures.

Summary

Combining 'Structured Layered Defenses aka Defense in Depth' through the incorporation of 1st and 2nd lines of defense is imperative for security architecture design. The 1st line serves as the primary barrier, actively preventing unauthorized access and reducing the attack surface. Meanwhile, the 2nd line acts as a robust backup layer, detecting and responding to threats that may breach the initial defenses. This dual-layered approach not only introduces redundancy and adaptability but also adds depth to the security architecture. The combination ensures a comprehensive and resilient defense strategy, effectively safeguarding against a diverse range of cyber threats and enhancing the overall security posture of an organization.

The ongoing practice of caring about security strengthens the overall organization's belief in its value, acting as a unifying force to improve security posture. The execution of the elements depends on the actions of every individual and organizational unit at all levels of the organization. Each of the elements can be expected to contribute to different aspects of the security culture, and these combined aspects reflect the strength of the culture. The RP, with all its discrete elements, supports the culture, and the culture feeds back into the management system in a continuous process, yielding an increasingly mature organization.

References

1. https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
2. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en
3. https://csrc.nist.gov/glossary/term/defense_in_depth

Revision	Date
Created Date	01-15-2024
Institute Date	01-22-2024
Published Date	01-22-2024

End of document.