ISAUnited
International Security Architects

Minimize Your Attack Surface-RP-215

Recommended Principle

Version 1-01.2024

www.isaunited.org

Forward

This guiding principle outlines the integration of ‘Attack Surface Management' into your 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

Minimize Your Attack Surface-RP-215

Recommended Principle

Version 1-01.2024

Description

The identification and comprehension of an organization's attack surface plays a important role in securing its defenses against potential threats. The attack surface constitutes the totality of potential entry points and vulnerabilities that could be exploited by malicious actors to compromise systems, networks, and applications. Understanding the attack surface is paramount for several reasons. Firstly, it provides a comprehensive view of the organization's potential weak points, allowing for targeted security measures. Secondly, a clear understanding of the attack surface facilitates effective risk management by enabling organizations to prioritize and address the most critical threats. Additionally, as technology evolves and organizations undergo changes, the attack surface dynamically shifts, emphasizing the need for continuous assessment and adaptation of security strategies. In essence, the identification of an organization's attack surface serves as a foundational step in developing a proactive and adaptive cybersecurity posture, essential for safeguarding against the ever-evolving landscape of cyber threats.

Scope

The attack surface scope consists of internet-facing assets of an organization's infrastructure and network components. Internet-facing assets, including web servers, applications, and network interfaces, represent the primary interfaces exposed to external entities. This encompasses securing exposed ports, validating user inputs, implementing robust access controls, and regularly assessing for vulnerabilities. At the foundation of this RP is the practitioners' existing architecture security posture. The requirements of this RP are comprehensive and define the elements needed to identify and address security for a practitioner's lifecycle. 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 must 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.

Attack Surface - Attack surface refers to the total of the possible entry points into a system. The attack surface is influenced by physical and network security, software, and computer security. Increasing the attack surface means increasing the potential for unauthorized access. The attack surface includes any potential entry points for malicious code to be smuggled into a machine via the internet, including email attachments, instant messages, and websites.

Attack Surface Management - In the context of ‘attack surface management’, the term ‘management’ refers to the ongoing process of identifying, assessing, and mitigating the various points of vulnerability and exposure within an organization's digital infrastructure. The attack surface of an organization consists of all the potential entry points, weak spots, and avenues that malicious actors could exploit to gain unauthorized access, steal data, or disrupt operations.

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

Discovery
In this phase, the goal is to comprehensively identify and catalog all potential entry points, assets, software, services, and connections that make up an organization's attack surface. This includes both internal and external elements. The process may involve automated scanning tools, asset inventory databases, network mapping, and manual assessments. The objective is to gain a clear understanding of the organization's digital footprint to ensure that nothing is overlooked.

Detect
Once the attack surface is identified, the next phase involves actively monitoring it for potential threats and vulnerabilities. This includes continuously scanning for new vulnerabilities in software, tracking changes to the organization's digital environment, and observing any anomalous activities that might indicate a security breach or an attempt at unauthorized access. Detection mechanisms may involve intrusion detection systems (IDS), intrusion prevention systems (IPS), security information and event management (SIEM) tools, and behavioral analytics.

Defend
The defend phase revolves around taking proactive measures to mitigate risks and protect the organization's digital assets. This includes addressing vulnerabilities, applying security patches, implementing access controls, and enhancing network segmentation. It also involves having incident response plans in place to swiftly react to any detected threats or breaches. Organizations may also employ threat intelligence feeds and security best practices to guide their defensive strategies.

These phases are not isolated actions; rather, they form a continuous loop of improvement and adaptation. As new technologies are adopted, systems evolve, and the threat landscape changes, the cycle repeats itself. Regularly discovering new potential entry points, diligently detecting emerging threats, and actively defending against vulnerabilities are key components of a robust Attack Surface Management (ASM) strategy.

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

Implementing 'Minimize Your Attack Surface' recommended principles strengthens an organization's security culture and posture. 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://csrc.nist.gov/glossary/term/attack_surface
2. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27400:ed-1:v1:en
3. https://www.cisa.gov/news-events/news/cisa-directs-federal-agencies-secure-internet-exposed-management-interfaces

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

End of document.