https://doi.org/10.70265/PNEZ3158

INTERNALS OF DEFENSE-IN-DEPTH STRATEGY IN CYBERSECURITY

Vladimir Babanov

Summary: *The current paper explores the fundamentals of the defense-in-depth strategy in cybersecurity, emphasizing its importance for threat response in the dynamic security landscape. By implementing multiple layers of independent security controls across physical, technical, managerial, and operational domains, organizations can effectively mitigate risks and prevent cyberattacks. The strategy's adaptability makes it a robust framework for addressing evolving cybersecurity challenges, offering a comprehensive method of protection against a wide range of threats.*

Key words: *defense in depth, cybersecurity, cybersecurity controls, threats, strategy*

INTRODUCTION

The security of digital assets might be compromised through a multitude of vectors. The multidimensional nature of threats and the vastness of the attack surface make the tailoring of a single solution to guarantee security impossible (Singer & Friedman, 2014). Hence, defenders need flexible, robust, and dynamic means that can also be adapted to their specific requirements in response to the threats and vulnerabilities in a constantly evolving cybersecurity landscape. Cyberspace has emerged as a new domain of competition between contemporary superpowers, especially between China and USA (Buyukliev, 2022), which further complicated the security environment globally.

The defense-in-depth strategy in the cybersecurity context contains all these traits, and its importance has been growing exponentially in recent years. This strategy proves highly effective in the multidimensional security environment as it integrates various security controls that complement one another in a way that allows their independent functioning. Preventing breaches and disruptions of any aspect of an organization’s activity is the main goal of a defense-in-depth strategy.

The objective of this article is to focus on two concepts: the defense in depth strategy and the cyber security frameworks and controls as critical means for its application. In particular, the research seeks to assess the layered security controls and measures taken to reduce risks and avert cyber assaults on the systems incorporating the physical, technical, managerial,

and operational domain. The subject of the study is the implementation of essential measures to implementing defense in depth strategy.

1. ESSENCE AND IMPORTANCE OF THE DEFENSE-IN-DEPTH STRATEGY

The cyberspace environment possesses extremely high degrees of uncertainty and unpredictability, which renders the search for security a constant effort rather than a state to be achieved. Planning, budgeting, implementation, monitoring, and changing tactics and procedures to defend a system have been in constant flux for the majority of entities with a solid online presence. Naturally, these ongoing fine-tuning efforts shouldn't be carried out arbitrarily without first analyzing the needs of an organization and reviewing the recommendations of the most reputable regulatory bodies.

Since the digital sphere encompasses all resources necessary to connect users online (Popov, 2020), establishing rules and regulations to protect these assets becomes vital.

Among the most significant organizations that provide regular recommendations about cybersecurity standards, baselines, controls, and more are the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). NIST has a number of significant documents that regulate frameworks on cybersecurity, privacy, risk management, AI risk management, and more.

Another fundamental NIST document that directly concerns the defense-in-depth concept is NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations (Joined Task Force, NIST, US Department of Commerce, 2020). In this document, NIST defines defense-in-depth as a security strategy that intertwines people, technology, and operations capacity to provide different obstacles across multiple stages inside an organization (Ibid., p. 401).

Important parts of ISO's contribution to establishing frameworks and baselines that refer to cybersecurity and could be used to develop a robust defense-in-depth strategy are ISO/IEC 27001:2022 and ISO/IEC 27014:2020.

The importance of the defense-in-depth strategy for cybersecurity stems from its ability to implement multiple dimensions of defense mechanisms that ensure maximum protection through independent security controls. This property aims at thwarting the intentions of malicious actors by breaching a system using different methods and tactics. The defense-in-depth approach possesses tremendous advantages considering the fact that cybersecurity concerns so much more than just logical aspects.

Its implementation starts with securing the physical infrastructure, which is a crucial aspect of defending cybersecurity. All systems require physical setups that make their functionality possible. Neglecting the

physical part of cybersecurity means such high exposure to risks that a breach would be inevitable.

Unauthorized access to assets on a logical level could also be prevented by a multitude of measures that include multifactor authentication, least privilege account policy, separation of duties and many more. The aim is not only to prevent an attack but also to mitigate insider threat attacks and the vertical movement of an intruder in a system (Stallings, 2011). Simultaneously mitigating threats at all levels by implementing various independent measures is the essence of the defense-in-depth strategy in cybersecurity.

The aforementioned NIST and ISO, though not exclusively, provide insight about the foundations of cybersecurity and the different frameworks and baselines that concern the defense-in-depth strategy. They outline the main factor with the greatest importance for implementing the defense-in-depth strategy in any organization: security controls.

2. SECURITY CONTROLS AS CRUCIAL PART OF THE DEFENSE-IN-DEPTH STRATEGY

Security controls are practical measures at all levels that are put in place with the goal of protecting the assets of an organization. There are sets of recommendations and minimum standards for the use and implementation of security controls, named baselines. The baseline is a pivotal starting point that could be subject to changes in accordance with the organization's specific needs.

The baseline may be adjusted by removing unnecessary recommendations or incorporating tailored measures to align with organizational needs. Some recommendations could also be customized or replaced to fit specific needs, or completely different ones to be added to the baseline recommendations. This circumstance illustrates the flexibility of the security controls and the many ways of their appliance into the defense-in-depth strategy in cybersecurity.

In a publication by the Center for Internet Security, a detailed list of security controls is displayed and separated by their various properties (CIS, 2024). The great number of security controls could be generally divided into four types- technical, managerial, operational and physical. Technical controls are implemented by using technical devices and hardware, as well as software or embedded firmware. Firewalls and encryption are examples of technical controls implemented by different ways.

Managerial controls include all measures implemented by the organization's management and policy and aim to proactively identify and mitigate risks. Risk management and project management are typical managerial controls. Operational controls are activities performed by personnel like specific training, testing, drills and others. The physical

controls are designed to address issues that involve physical interaction with an organization's assets. The physical controls include fences, gates, locks, etc.

Due to their variety and sheer number, the security controls could also be divided into different categories, which helps with their classification. A security control might also possess traits of different types and categories, depending on the context of their usage. The main categories of security controls are deterrent, aiming to discourage an attacker, preventative that aims to stop an attack, detective which detects and reports attackers, and corrective which minimizes the impact of a threat.

All entities could combine different controls in a suitable way so the end result could be a unique cybersecurity program, containing aspects unseen elsewhere. Even if based on the broad recommendations of the recognized bodies in the field, the implementation of defense-in-depth should lead to a unique cybersecurity stance for any organization, resulting in custom intrusion detection and prevention systems, threat intelligence program and many more.

3. SOME CONSIDERATIONS FOR IMPLEMENTING THE DEFENSE-IN-DEPTH STRATEGY

Among the most important aspects to consider is the topology of the network and the possible ways for its segmentation. Although not always necessary, breaking a network down into different areas could be helpful in limiting the damage a hacker could inflict, in case of a breach or infiltration. Properly dividing a network requires meticulous planning and setting up in order to safeguard adequately the various segments.

Another factor that is considered an important aspect of defense-in-depth is the use of Intrusion detection systems (IDS) and Intrusion prevention systems (IPS). Thus, these systems allow observation of the activity in the network traffic and detecting potential security issues within a short time frame as well as preventing unwanted traffic into the organization's network (Scarfone & Mell, 2007).

Without proper fine tuning of the IDS and IPS, an organization is running a risk of various discrepancies in the actual state of the system and the alerts it has been given by the IDS and IPS. It is therefore recommended to carry out periodic tests of the IDS and IPS to ascertain the functionality of the adopted systems, and its ability to detect threats correctly as well as not ignoring the human role in their management and usage.

Endpoint security is another measure of defense in depth aiming for protection of data on the occurrence of malware and unauthorized access on a particular client. It is implemented to safeguard individual computers, laptops and other portable devices, including in physical aspect. It enables users the ability to secure their data and information, for example personnel

and patients' data, across different platforms through different approaches. There are various baselines and procedures for ensuring the security of devices in a network.

CONCLUSION

Defense-in-depth is an important approach to cyber security and it helps in addressing the complex, ever changing nature of threats and vulnerabilities in cyberspace. The end result is the implementation of multiple security controls that are interdependent while capable of operating independently. This approach looks forward to pre-empting possible breaches and disruption throughout all areas of business operation. Organizations often rely on guidelines from the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO) for cybersecurity standards, baselines, and controls.

The defense-in-depth strategy focuses on safeguarding physical infrastructure, preventing unauthorized asset access, as well as minimizing insider threat attacks. It is necessary to have security controls at every level in order to protect an organization's properties. Customization may be required for minimum standard or baseline guidelines according to individual needs.

There are four main types of security controls which are categorized into technical, managerial, operational and physical. Such can be classified under deterrents, preventives, detectives and correctives respectively. Forcing network topology considerations into a defense-in-depth implementation include network segmentation or enclave boundaries among others.

Defense-in-depth remains one of the best concepts to protect assets in the digital realm due to its adaptability that makes it possible for organizations to tailor security for their unique needs. As the cyber threats evolve further, it is safe to say that the concept of defense-in-depth will continue to be a crucial model in risk mitigation within the entire scope of the digital ecosystem.

BIBLIOGRAPHY:

Буюклиев, Е. (Декември 2022). Стратегическото съперничество между САЩ и Китай през XXI век. *Сигурност и отбрана,* (2), 223-239. https://institute.nvu.bg/sites/default/files/inline-files/2022-2-13-buyukliev.pdf // Buyukliev, E. (Dekemvri 2022). Strategicheskoto sapernichestvo mezhdu SASHT i Kitay prez XXI vek. *Sigurnost i otbrana,* (2), 223-239. https://institute.nvu.bg/sites/default/files/inline-files/2022-2-13-buyukliev.pdf

Попов, Н. (2020). Дигиталните компетенции в политическата система. В Андонов, В. и др. (Ред.), *Научни трудове на Съюза на учените в България – Пловдив. Серия А. Обществени науки, изкуство и култура, Том VI* (с. 83-86). https://usb-plovdiv.org/wp-content/uploads/2020/06/2020_obshtestveni_nauki_tom_VI.pdf // Popov, N. (2020). Digitalnite kompetentsii v politicheskata sistema. V Andonov, V. i dr. (Red.), Nauchni trudove na Sayuza na uchenite v Balgariya – Plovdiv. Seriya A. Obshtestveni nauki, izkustvo i kultura, Tom VI (s. 83-86). https://usb-plovdiv.org/wp-content/uploads/2020/06/2020_obshtestveni_nauki_tom_VI.pdf

Center for Internet Security (CIS). (August 2024). *CIS Critical Security Controls (v8.1)*. Retrieved September 18, 2024, from learn.cisecurity.org/cis-controls-v8-1-guide-pdf

Joint Taks Force. (2020). *Security and Privacy Controls for Information Systems and Organizations* (NIST SP 800-53, Rev. 5). National Institute of Standards and Technology (NIST), US Department of Commerce. Retrieved August 29, 2024, from https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (n.d.). *Frameworks*. NITS. Retrieved August 29, 2024, from https://www.nist.gov/frameworks

Scarfone, K., & Mell, P. (February 2007*). Guide to Intrusion Detection and Prevention Systems (IDPS)* (NIST SP 800-94). National Institute of Standards and Technology (NIST), US Department of Commerce. Retrieved August 29, 2024, from https://doi.org/10.6028/NIST.SP.800-94

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know* [eBook edition]. Oxford University Press. Retrieved September 20, 2024, from https://books.google.bg/books?id=9VDSAQAAQBAJ&printsec=frontcover&hl=bg#v=onepage&q&f=false

Stallings, W. (2011). *Network Security Essentials: Applications and Standards* (4th ed.) [eBook edition]. Pearson Education. Retrieved September 20, 2024, from https://elhacker.info/manuales/Redes/3._Network-security-essentials-4th-edition-william-stallings.pdf