ISBN: 978-981-18-3959-7
2022 the 12th International Workshop on Computer Science and Engineering (WCSE 2022)
doi: 10.18178/wcse.2022.06.046

PPDRRF: A Feasible Model for Construction of Cybersecurity Systems and Its Application

Lanjun Li [1, 2+], Zhongyi Liang [1] Xiaodong He [2] and Baohong Ling [1]

[1] School of Information Engineering, Anhui broadcasting Movie and Television College, Hefei, 230011, China

[2] Network and Information Center, Anhui broadcasting Movie and Television College, Hefei, 230011, China

Abstract. By analyzing the PDR, P2DR, P2DR2 model and the techniques it uses, this paper innovatively adopt RIO (Rate of Input and Output on cybersecurity) in the PPDRRF (Policy, Protection, Detection, Response, Recovery and Forensic) model, and quantitatively analyzes some key technologies of cybersecurity system construction, proposes Cybersecurity System Architecture (CSA) and ensures the smooth progress of cybersecurity construction under resource constraints. Finally, we applied PPDRRF in CSA and realized it in the campus network.

Keywords: network security; classified protection 2.0; Return On Investment; RIO; P2DR; CSA

1. Introduction

With the enforcement of Cybersecurity Law of the People's Republic of China [1] (referred to simply as the Security Law), as the network provider of the campus network, universities need to take the responsibility of protecting the legitimate use of the campus network. Current campus network is a huge and complex system, which supporting the business operation and development of universities. Cybersecurity threats faced by information systems are also growing, more and more vulnerabilities or weaknesses are found, and information security risks are becoming increasingly prominent, becoming one of the important and urgent problems. On the other side of the coin, universities often fall into the embarrassing situation of shortage of human resources, financial resources and equipment when cybersecurity problems happening.

A time-based security model ANSM (Adaptive Network Security Model) was proposed in the 1990s, which is also called P2DR (policy protection detection response) model. Based on the best practices and P2DR model, the NSA released the Community Gold Standard v2.0 (CGS2.0) in June 2014, which provides a holistic view of Information Assurance (IA) considerations for decision makers to efficiently plan since then. The CGS2.0 standard framework emphasizes the four overall functions of cyberspace security: govern, protect, detect, respond and recover [2]. At present, most of the research on network security system agree with the comprehensive and dynamic protection [3], but the design of cybersecurity protections only emphasizes large and comprehensive, and does not consider the cost of systematic protection. It is very urgent to propose a feasible model for construction of cybersecurity systems.

2. PPDRRF

2.1. PDR

In the 1990s, Winn Schwartau proposed the PDR network security model, which describe a network security solution from the aspects of Protection, Detection, and Response [2]. The time relationship between protection, detection and response is given, and the formula is Pt>Dt+Rt, which creates a time-based network security protection model. The protection includes the formulation of security rules, the configuration of system security, and the adoption of security measures. The detection includes two aspects of anomaly

+ Corresponding author. Tel.: +86-0551-64200345
E-mail address: lilanjun@amtc.edu.cn.

monitoring and pattern discovery, and the response includes four aspects: reporting, recording, reaction, and recovery.

2.2. P2DR

In the late 1990s, the American ISS proposed P2DR (policy, protection, detection, response) model. P2DR adds Policy [2] based on PDR, which is also one of the most classic models among all network security models. Policy includes monitoring period setting, recovery mechanism, and access control strategy. The P2DR model also adds a formula Et = Dt+Rt (if Pt = 0) on the basis of the PDR model, which means that if the protection time Pt is 0, then the detection time Dt and the response time Rt should be equal to the time the system is exposed to the network Et .

2.3. P2DR2

The domestic network security community has added Restore based on P2DR, and proposed the P2DR2 (Policy, Protection, Detection, Response, Restore) model [3], that is, the rapid restoration of the system based on reliable backup. The P2DR2 model is a dynamic network security model based on active defence and loop control. By analysing and formulating security policies, the model establishes a unified detection and monitoring mechanism within the network, and applies various types of disaster recovery and backup system redundancy design and other technologies, can realize the functions of resisting attacks, detecting attacks and restoring network data in a timely manner.

2.4. PPDRRF

The PPDRRF model we introduced is a dynamic, adaptive security processing model that can adapt to changing security risks and security requirements and provide continuous security assurance. The PPDRRF model includes six main parts: Policy, Protection, Detection, Response, Recovery and Forensic, shown as Figure 1.

Fig.1: PPDRRF model

Policy: In PPDRRF model, protection, detection, response, recovery, and forensics constitute a complete and dynamic security cycle, which together realize security assurance under the guidance of security policies. For the cybersecurity policy, we proposed idea of "three stages - four levels - one penetration", in which "three stages" refer to the design and development stage, deployment and implementation stage, and management and maintenance stage; "four levels" refer to the Application-level security, system-level security, network-level security and physical-level security; "one penetration" means that security management runs through the life cycle of the entire information system, and also runs through the "three stages" and "four levels".

Protection: The key goal of the protection is to reduce the attack surface and reduce losses before the cyber-attacks affect the network system. This phase typically includes operating system security configuration, vulnerability fixes, anti-Distributed Denial of Service (DDos), Intrusion Prevention System (IPS), firewall/next generation firewall, Web Application Firewall (WAF) and other cybersecurity products or technology.

Detection: This phase is continuously detecting network system has been compromised or there is a possibility of being compromised. The use of analytical tools can provide detection capabilities, such as Intrusion Detection System (IDS), vulnerability scanning system, web security monitoring system, network traffic analyser, Advanced Persistent Threat (APT) analyser, situation awareness, et al.

Response: This phase is to deal with discovered attacks timely and determine the root cause to avoid similar events in the future. A common approach is to analyse cybersecurity logs and adjust the security

system rules or add a new cybersecurity product in network. Automatic linkage with situational awareness is a way.

Recovery: This phase is restoring the system to ensure the availability and continuity. It usually includes data recovery and business recovery. Daily backup is necessary which includes scheduled backup, real-time backup, and recovery takeover when disaster occurs. Backup all-in-one is a solution that can be considered, which includes document backup, database backup, and configuration backup. Regular disaster recovery drills are also a recommended strategy.

Forensic: If the system has been compromised, forensic is the last countermeasure. The main goal of forensic is keeping logs as detailed as possible. The logs include operating system logs, database logs, middleware logs, application logs, network behaviour logs, operation logs, et al. Comprehensively standardize network logs, security logs, host logs, and application system logs to discover various security threats is the key function of big data cybersecurity audit system.

The PPDRRF model contains many network security technologies and products as mentioned above. How to choose specific security countermeasures economically? Next, we analyse countermeasures from an economic point of view.

3. Analysis of Countermeasures

Return on investment (ROI) is a performance measure used to evaluate the efficiency of an investment or to compare the efficiency of several different investments [4]. The Return On Investment formula:

$$ROI = \frac{Net\ Profit}{Cost\ of\ Investment} \times 100\% \quad (1)$$

ROI refers to the economic return of an enterprise from an investment, but investment on cybersecurity do not expect a profit return. Therefore, the calculation of the ROI of cybersecurity should be how much loss was avoided through the security investment, also known as ROSI (Return On Security Investment) [5], ROSI is calculated as follows

$$ROSI = \frac{\text{Reduced Loss} - \text{Cost of security measures}}{\text{Cost of security measures}} \times 100\% \quad (2)$$

At present, there is no uniform standard for Reduced Loss [5]. ALE (Annual Loss Expectancy) was introduced, which considering Asset value, level of damage, ARO (Annual Rate of Occurrence). ALE is the loss caused by the annual cyber-attack, which refers to the potential loss that cyber-attack may cause to the company or organization in one year, calculated as ALE = ARO*SLE. ARO is the probability that a cybersecurity incident will occur in a year, that is, the probability and number of times a certain cyber threat may occur in a year. SLE (Single Loss Expectancy) is loss expectancy caused by the occurrence of a cyber-attack alone. However, the particularity of cyber threats is relatively complicated when calculating losses, such as a notebook lost, regardless of the value of the notebook, but also to add the cost of purchase, IT support, loss of productivity, reputation, intellectual property loss and so on. ROSI calculation relies on the monetization calculation of losses. ROI calculation relies on the monetization calculation of income, and the monetization calculation of network security income or loss often depends on the definition of income and loss of specific individuals, this assessment is based on the specific network environment and security protection measures, but also based on experience to obtain an estimate, so the implementation process often causes the calculation results to be inconsistent [5]. Therefore, we need a new feasible method to calculate return on cybersecurity system, which contains all factors above, such as protected asset value, potential loss, rate of occurrence, reduced loss, etc.

According to GB/T 22239-2019 [6], The core of classified protection of cybersecurity (also known as classified protection 2.0) is using key information infrastructure to protect the security of the cyberspace, levelled by protected asset value and the destruction consequences of cyber-attacks. When a level 2 system is evaluated by classified protection 2.0, for example, it is assigned a score according to the implementation of security countermeasures. Reference [7] and [8] detail how to obtain this score. The score is a feasible indicator of return on cybersecurity investment, which can be used as Net Profit in formula 1. We call the score CPS (Classified Protection Score) in this paper:

$$CPS = \begin{cases} INT(score), & score \geq 70 \\ 0, & score < 70 \end{cases} \quad (3)$$

The level of classified protection 2.0 is divided according to the importance of the evaluated system and the destruction consequences, and the qualifying score is 70 points (out of 100) [7]. So, when the score is less than 70, CPS is directly equal to 0, Otherwise CPS is the rounding of the score. In other words, the calculation factor of CPS already includes protected asset value, potential loss of asset, rate of occurrence and reduced loss. CPS is the Net Profit or output of cybersecurity system construction.

We propose the concept of RIO (Rate of Input and Output on cybersecurity). Input on cybersecurity is cost of countermeasures, and output on cybersecurity is CPS. RIO is the reciprocal of ROI in formula 1. The RIO proposed calculation formula is:

$$RIO = \frac{Cost\ of\ \ countermeasures}{CPS} \quad (4)$$

Cost of countermeasures is obtained from median of security vendor quotes corresponding security measures, CPS is calculated according to formula 3. RIO is combined with the advantages of ROI in formula 1 and ROSI in formula 2. The smaller the RIO, the better the security countermeasures.

As a key information infrastructure of classified protection 2.0, we take malicious code prevention as example, the calculation of RIO is shown in Table 1:

Table 1: An Example of Rio

Category	**RIO=Cost/CPS**			
	countermeasures	**Cost(￥)**	**CPS**	**RIO**
Malicious code prevention	free antivirus software	0	0	∞
	Centralized antivirus software	20000	76	253.16
	Antivirus firewall	25000	77	324.68
	Antivirus Software & firewall	45000	78	576.92

As a level 2 evaluation object of classified protection 2.0, website “www.amtc.edu.cn” was found 28 cybersecurity issues. A total of 135 evaluation indicators were selected. The overall score for the evaluation was 77.97. The security measures we used in the first evaluation were antivirus firewall plus centralized antivirus software. Now we use alternative countermeasures in the malicious code prevention category and bring it into the scoring system. Finally, the score is rounded or zeroed to get the CPS. The calculation results are shown in Table 1.

In Table 1, RIO minimum value 253.16 corresponds to “Centralized antivirus software”, so the most cost-effective countermeasure in the malicious code prevention category is centralized antivirus software. In a similar way, we got the most cost-effective countermeasures in the key categories of classified protection 2.0.

According to this idea, we can design our cybersecurity system architecture.

4. Application of PPDRRF

As mentioned above, we identify the most critical layers of cybersecurity protection and proposed Cybersecurity System Architecture (CSA) drawing on PPDRRF model. Based on the baseline for classified protection of cybersecurity [6], CSA has four lines of cybersecurity defense and security management center, combining the PPDRRF model., shown as Figure 2.

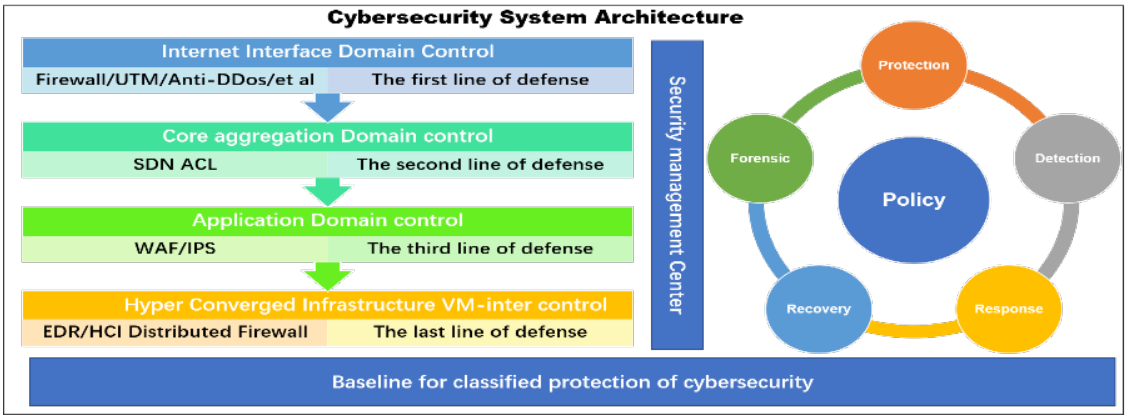

Fig.2: Cybersecurity System Architecture (CSA)

In CSA, we followed the basic idea of classified protection 2.0, which is featured by "one center and three lines of defense" [6]. The protective measures taken can meet the requirements of the PPDRRF model.

- The first line of defense: The first line of defense mainly realizes internet interface domain control. We deploy a next-generation firewall at the entrance of the campus network as the first line of defense for cybersecurity. The firewall explicitly deny access to high-risk ports, such as 1433, 445, 135-139, et al. in the access control list, and set highest priority to avoid unintentional accept in the later maintenance process. The list of high-risk ports changes dynamically. When a new worm breaks out, the ports will be dynamically added to the list. The firewall policy is set to deny by default, allowing only necessary ports such as websites and campus apps. The next-generation firewall integrates anti-distributed-denial-of-service (DDos) implementing the functions of protection and response in the PPDRRF model.
- The second line of defense: The second line of defense mainly realizes core aggregation domain control. With the help of SDN technology, we add access control list (ACL) to the core switch to control traffic between VLANs. According to statistics, 80% of network attacks originate from the internal network [3]. Therefore, it is necessary to strengthen the security control and prevention of the internal network. In addition to the first line of defense, the remaining lines of defense are both internal and external. Departments with different VLANs are divided into security areas. Traffic between different VLANs must pass through the core switch, so that ACLs applied to different VLANs can block high-risk behaviors such as virus outbreaks and hacker jumping. Even if some terminal poisoning occurs, the virus can be controlled within a certain range, providing time for the next step to quickly determine, isolate and deal. In the core switch, by mirroring the traffic to the behavior audit equipment, the functions of protection, response and forensics in the PPDRRF model are realized.
- The third line of defense: The third line of defense mainly realizes application domain control. We deploy a web application firewall (WAF) integrated Intrusion Protection System (IPS) function at the boundary of the server area. Through the filtering of the first and second lines of defense, the traffic entering the server area is mainly business traffic, but application layer attacks such as SQL injection and cross-site scripting (XSS) also follow. WAF can go deep into application layers to detect and block the attacks. Because it is deployed at the boundary of the server area, in addition to external attacks from the Internet, WAF can also block application layer attacks from inner area, and realize the functions of protection, detection, response and forensics in the PPDRRF model.
- The last line of defense: The last line of defense mainly realizes Hyper Converged Infrastructure (HCI) VM-inter control. With the advancement of virtualization, the server area of the campus network has been moved into the private cloud, and the servers communicate through the virtualized network. Server-to-server communication traffic inside a private cloud, we call it east-west traffic. If a server is compromised, the entire server zone will be compromised. In order to avoid this situation, we enable distributed firewall in the virtualized network. and installed centralized antivirus software “Endpoint Detection and Response (EDR)” for antivirus, OS security configuration and system patch

updates. EDR and HCI distributed firewall block the transmission of VM-inner and VM-inter malicious traffic, and realize the functions of protection, detection, response, recovery and forensics in the PPDRRF model.

- Security management center: Security management center mainly realizes security management. Cybersecurity situation awareness system, vulnerability scanning system, data recovery system and audit system are deployed here. Through security management, we can regularly analyse the security logs generated by each line of defense, scan security vulnerabilities， dynamically adjust the strategies of related security devices in the lines of defense, implement the security management system formed by the guidance of security strategies, and protect against new attacks such as APT, and realize the functions of policy, detection, response, recovery and forensics in the PPDRRF model.

At present, the data center of our college has deployed a HCI platform to form a private cloud. The campus network has deployed next-generation firewall, SDN, WAF, EDR, vulnerability scanning system, network behavior audit system and Cybersecurity situation awareness system, involving security vendors including Sangfor, venustech, dbappsecurity, Topsec, H3C, et al, fully considering the heterogeneous type of network security defense lines, and the defense lines cooperate with the security management system to form the campus network CSA.

For the effect of CSA, we randomly select a week as an example (here, we select a full week from March 20 to 26, 2022), and the amount of web attacks blocking logs is used as the statistical result. The first line of defense records the number of logs blocked by next-generation firewall, the third line of defense records the number of logs blocked by WAF, and the last line of defense records the number of logs blocked by EDR, as shown in Table 2. (Due to performance reasons, the security equipment used in the second line of defense cannot enable the log function, and not be recorded here)

Table 2: Amount of logs blocked by the Lines of defense

date	**3.20**	**3.21**	**3.22**	**3.23**	**3.24**	**3.25**	**3.26**
Logs blocked by First Line	147166	124985	138734	103269	845322	45206	153644
Logs blocked by Third Line	733	751	625	742	8071	779	1405
Logs blocked by Last Line	153	63	26	67	56	225	19

In theory, all web attacks should be blocked before the third line of defense, which are built on traditional security model, and the log volume of the last line of defense should be 0. But in fact, as the last line of defense linked with the security management center, a small number of blocking logs are generated almost every day. After analysis, the special structure of attack traffic can bypass the protection rules before the third line. The logs generated by the last line of defense demonstrated effectiveness of CSA. We finally passed the evaluation for classified protection 2.0 of cybersecurity at a relatively small cost.

5. Conclusion and Future Work

In this paper, we proposed RIO in the PPDRRF model and designed Cybersecurity System Architecture (CSA). Referred to the baseline for classified protection of cybersecurity, CSA has four lines of cybersecurity defense and security management center. Finally，we constructed four lines of defense and security manager center to implement CSA.

However, the calculation of RIO may be inconsistent, cost of countermeasures in formula 4 is obtained from median of security vendor quotes, which fluctuates greatly from vendor to vendor. Therefore, in the future we will focus on optimizing the calculation of cost of countermeasures, one of the directions is to obtain data from bidding online for big data analysis.

6. Acknowledgements

This work is supported by Anhui Province Higher Education Natural Science Research Project (KJ2019A1145) and Teaching Team of Computer Network Technology Project(2020jxtd050).

7. References

[1] “Cybersecurity Law of the People’s Republic of China” http://www.npc.gov.cn/npc/, 2016-11-7.

[2] Wang Yan, Sun Degang, Lu Dan. American Network Security Architecture. Journal of information Security Research,2019,5(07):582-585.

[3] PAN Shanhai, PEI Hua. Research and design of high security level network security protection system. Communications Technology,2021,54(7):1715-1720.

[4] https://byjus.com/commerce/what-is-return-on-investment/

[5] Daniel Schatz and Rabih Bashroush. "Economic valuation for information security investment: a systematic literature review". Information Systems Frontiers 19.5(2017): 1205-1228.

[6] GB/T 22239-2019. “Information security technology — Baseline for classified protection of cybersecurity”. Beijing: Standards Press of China,2019.

[7] GB/T 28448-2020. “Information security technology —Evaluation requirement for classified protection of cybersecurity”. Beijing: Standards Press of China,2020.

[8] Xin Jiang, Yanqing Ding, Xiudan Ma, Xumao Li, Compliance analysis of business information system under classified protection 2.0 of cybersecurity, Procedia Computer Science, Volume 183,2021, Pages 87-93