Postprint: Technical Protection and Management of Network Security in Grassroots Public Institutions

Authors: Zhang Zhiwei

Date: 2023-10-08T00:00:00+00:00

Abstract

Driven by the continuous wave of network informatization, network scale has expanded rapidly, with various industries actively integrating into this digital ecosystem. The resulting Internet economy has not only facilitated enterprise development but also fundamentally transformed people' s lives. However, concomitant network information security issues have become increasingly prominent. Due to the inherent vulnerabilities of networks, problems such as hacker attacks and virus proliferation have emerged incessantly, posing threats to network security and potentially causing significant harm. Therefore, while enjoying the convenience afforded by networks, we must maintain heightened vigilance regarding network security issues. This paper elaborates on the network security challenges confronting grassroots public institutions and corresponding protective measures, encompassing both technical prevention and security management, aiming to preempt potential network security risks and further enhance the security and reliability of computer networks in grassroots public institutions.

Full Text

Cybersecurity Technical Protection and Management in Grassroots Public Institutions

Abstract: Driven by the wave of network informatization, network scale has expanded rapidly, with various industries actively integrating into the digital ecosystem. The resulting internet economy has not only propelled enterprise development but also transformed people' s lives profoundly. However, accompanying network information security issues have become increasingly prominent. Due to inherent network vulnerabilities, problems such as hacker attacks and virus proliferation emerge endlessly, posing threats and potential hazards

to network security. Therefore, while enjoying the convenience brought by networks, we must maintain high vigilance regarding security issues. This paper expounds on the cybersecurity challenges faced by grassroots public institutions and corresponding protective measures, encompassing both technical prevention and security management, aiming to avoid potential network security risks and further enhance the security and reliability of computer networks in grassroots public institutions.

Keywords: grassroots public institutions; network security; security protection

Author: Zhang Zhiwei

1.1 Definition of Network Security

The International Organization for Standardization (ISO) document 7498-2 defines security as maximizing the reduction of possibilities for data and resources to be attacked. Article 3 of the *Regulations on the Security Protection of Computer Information Systems of the People' s Republic of China* standardizes the concept of security for computer information systems, including computer network systems: the security protection of computer information systems shall ensure the safety of computers and their related and supporting equipment and facilities (including networks), the security of the operating environment, the security of information, and the normal functioning of computer functions to maintain the safe operation of computer information systems.

1.2 Basic Elements of Network Security

Essentially, network security means protecting network system hardware, software, and data from being destroyed, altered, or disclosed due to accidental or malicious attacks, ensuring that systems can operate continuously, reliably, and normally without interruption of network services. Broadly speaking, all technologies and theories related to the confidentiality, integrity, availability, controllability, and non-repudiation of network information constitute the field of network security research. These are the five fundamental elements of network security. Confidentiality primarily ensures that unauthorized users cannot access information and that information is not exposed to unauthorized entities or processes. Integrity ensures that only permitted users can modify entities or processes. Availability ensures that authorized users can access information at any time, with access control mechanisms preventing unauthorized access. Controllability refers to having authorization mechanisms to control information dissemination behavior, content, and scope. Non-repudiation means that security incidents can be monitored and audited, ensuring traceability.

Network security and openness exist in a contradictory relationship. A system that provides no services generates no security threats; once services are provided in an open network environment, various security issues inevitably follow.

2.1 Inherent Defects in Network Protocols

Network communication protocols form the foundation of internet transmission. When these protocols were initially designed, the complexity of modern networks was not anticipated, resulting in various native defects. TCP/IP is the fundamental protocol of the Internet, and numerous attack methods exploit its vulnerabilities. Physical layer attacks primarily involve physical destruction of network hardware and infrastructure. For example, construction work that damages power lines causing power outages, or severed exit cables, can both result in loss of internet access. ARP (Address Resolution Protocol) and RARP (Reverse Address Resolution Protocol) are two important protocols at the TCP/IP data link layer, where ARP spoofing and impersonation are common attack methods. The network layer includes ICMP, IP, and IGMP protocols, which frequently give rise to notorious network attacks such as ICMP routing deception, Smurf attacks, and IP fragmentation attacks. The transport layer is a heavily attacked area, with numerous attack scenarios resulting from TCP' s resource-intensive connections, slow release, and UDP' s connectionless, unreliable nature, including session hijacking, man-in-the-middle attacks, SYN flood attacks, and TCP sequence number deception and attacks. At the application layer, numerous application protocols exist, such as DNS, FTP, and SMTP, with DNS spoofing being the primary attack vector. Additionally, vulnerabilities in software such as databases and self-developed applications can also attract hacker attacks.

2.2 Hazards of Malicious Code

Due to the open and interconnected nature of networks, users can freely move between various sites, and information systems interconnect with each other, making user identity and location difficult to identify. Simultaneously, technical vulnerabilities in network protocols and some software provide convenience for the propagation and diffusion of malicious code. Common threats such as malicious worms, viruses, buffer overflow code, and backdoor Trojans exploit defects in TCP/IP protocols. An increasing number of severe attack incidents demonstrate that the current cybersecurity situation is grave, with criminals constantly updating their techniques. Network administrators must continuously monitor security vulnerabilities, and cybersecurity prevention measures must keep pace with evolving threats to ensure network information security and controllability.

2.3 Human Factors

Many computer users lack cybersecurity awareness and engage in improper usage practices, making them susceptible to risks such as extortion and ransomware through unsafe websites or emails that implant Trojan backdoors. These human factors also contribute to security incidents.

3.1.1 Physical Security

Physical security protects computer network equipment, facilities, and other media from environmental accidents such as earthquakes, floods, and fires, as well as from human operational errors or various destructive acts targeting networks or computers. Ensuring the physical security of various devices in computer information systems is the prerequisite for overall computer information system security. Physical attacks can be accidental or intentional. Intentional attacks involve obvious destruction of network physical cables, equipment, or supporting facilities that render network services unavailable. Accidental incidents differ in nature from intentional attacks but produce the same result —damage to networks or specific equipment. Accidental incidents may not be classified as attacks. Physical environmental security primarily refers to the protection of system and equipment rooms. Protective measures and procedures should be implemented according to relevant national design standards, including fire alarms, safety lighting, uninterruptible power supply, temperature and humidity control systems, and anti-theft alarms, all of which should comply with national design specifications for different levels of computer rooms.

3.1.2 Network Boundary Security

Network security primarily encompasses the security of network operations and access control. Deploying firewalls between internal and external networks to isolate and control access to external networks represents the most important and cost-effective measure for protecting internal network security. Firewalls can be categorized by implementation principle into packet-filtering firewalls, application-level gateway firewalls, proxy firewalls, and rule-checking firewalls, with their deployment locations entirely dependent on organizational access and security requirements. Objectively speaking, firewalls are not a panacea for network security problems but rather one component of network security and strategy. Firewalls have many limitations, such as their inability to prevent attacks that exploit protocol defects or address security issues originating from internal networks. Therefore, relying solely on firewalls at internet entry points cannot protect the entire internal network; specialized security equipment such as IPS (Intrusion Prevention Systems) should also be deployed to compensate for firewall deficiencies. Positioned between firewalls and network devices, IPS can configure deep-level defense security policies, monitor network transmissions, and adjust or block abnormal transmissions through packet inspection—capabilities that firewalls cannot provide. As an essential network security addition, IPS has become standard equipment in most organizational network security architectures.

3.1.3 Integrated Terminal Security and Unified Prevention

In the current internet environment, most grassroots public institutions have established complete network platforms with considerable scale and numerous computer terminals. Various new attack methods such as Trojans, viruses, zero-

day vulnerabilities, and APT-like attacks are proliferating, rendering traditional antivirus technologies and management approaches insufficient for current cybersecurity needs. Establishing an integrated terminal security and unified network threat protection system has become the preferred choice for organizations to defend against cybersecurity threats holistically. The vast majority of domestic cybersecurity companies offer network security management systems for enterprise and institutional users. Relying on their respective cloud security systems, these solutions provide comprehensive assessment of network terminal security status, thorough detection and elimination of known and unknown viruses and malicious code, real-time security patch updates through cloud security, and adjustment of threat protection strategies. Through security auditing and tracking of network files, unknown threats can be detected and located promptly, with terminal vulnerabilities repaired and patches automatically pushed, maintaining network terminal security risks in a manageable and controllable state. Simultaneously, these systems can digitally display the overall security status and risk conditions of network terminals, helping cybersecurity administrators understand terminal risk situations promptly, accurately, and clearly to facilitate rapid problem resolution.

3.2 Management Measures

Through years of research and practice in the cybersecurity field, people have gradually recognized the importance of management in network security, with the concept that "management accounts for seven parts while technology accounts for three" becoming deeply rooted. Network security also follows the "barrel principle" —the capacity of a barrel depends on its shortest stave, and a system' s security strength equals that of its weakest link. Regardless of how advanced the technical equipment employed, management measures targeting human factors are necessary for support. As long as vulnerabilities exist in security management, the system' s security cannot be guaranteed.

3.2.1 Regular Network Monitoring

Network status is constantly changing, and the threats facing network computers also evolve with the network environment. Network administrators' job responsibilities and daily work should be institutionalized, including regular inspection of virus signature updates on networked computers to ensure they remain current, enabling anti-closing and anti-uninstallation functions of terminal protection programs, and frequently checking terminal security status within the network through integrated terminal management systems. Security detection commands should be proactively pushed to intranet terminals for automatic vulnerability patching when powered on. For internal computer networks, input and output should be strictly controlled, with identity-based encrypted access technology employed when necessary to authenticate visitors and confirm access permissions—an effective method for maintaining network security. Additionally, network administrators should regularly employ cyber-

security monitoring tools such as malware analysis packages, network traffic analysis tools, port scanning tools, and vulnerability detection frameworks to detect system vulnerabilities or potential threats, patching them promptly to enhance network security.

3.2.2 Strengthening Internal Management and Security Awareness

Although grassroots public institutions have relatively fixed and simple personnel structures, this does not guarantee that computers used within the internal network are secure. Cybersecurity threats originate both externally and internally. Grassroots units typically lack dedicated cybersecurity management personnel and have relatively weak defense capabilities. First, technical training for network administrators should be strengthened to effectively supplement new cybersecurity management knowledge and improve cybersecurity prevention skills. Additionally, units should conduct irregular annual cybersecurity self-inspections, summarizing existing security risks in network usage and conducting various forms of cybersecurity education activities using relevant case studies. Particularly, staff security awareness should be enhanced, restraining curiosity and avoiding clicking on suspicious emails and links to prevent cybersecurity incidents such as Trojan implantation, extortion, and fraud. Employees should be cultivated to develop good habits of scanning mobile storage devices before use and encouraged to use legitimate software, as pirated software inherently contains certain security threats. Simultaneously, supervision mechanisms must be improved to ensure these systems are effectively implemented; otherwise, network security cannot be guaranteed.

Cybersecurity prevention is a dynamic process. Factors affecting security are constantly changing, and prevention must consequently be implemented through a dynamic process. A reliable network security guarantee system should not only effectively defend against external attacks but also include comprehensive internal security management systems. It should not be limited to preventing specific security risks but should possess holistic capabilities to address various network security threats, continuously improving and perfecting itself as security requirements evolve. This requires network administrators in grassroots public institutions to strengthen comprehensive network monitoring in their daily work, carefully observe and analyze factors affecting network security, reinforce secure usage management of internal computers, eliminate potential security risks to the greatest extent possible, and ensure the stable, reliable, and orderly operation of computer networks in grassroots public institutions.

References: [1] Shi Shuhua, Chi Ruinan. *Computer Network Security Technology* (4th ed.) [M]. Posts & Telecom Press, 2016: 5-6. [2] Jacobson D. *Fundamentals of Network Security: Network Attack and Defense, Protocols and Security* [M]. Translated by Yang Liyou, Zhao Hongyu. Publishing House of Electronics Industry, 2016: 262-270. [3] Chen Xiaohua, Wu Chuankun. *Network Security Technology: A Guarantee for the Healthy Development of Cyberspace* [M]. Posts & Telecom Press, 2017: 27-28.

Author Affiliation: Xinhua News Agency Beijing Branch

Note: Figure translations are in progress. See original paper for figures.