Frontiers in Power and Energy Systems (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/fpes.2024.030105
ISSN 2516-2926 Vol. 3 Num. 1

New Technologies in Active Defense and Their Application in Electric Power Information Network Security

Cong Wang

State Grid Shandong Electric Power Company Information and Communication Company, Jinan, Shandong, 250000, China

Keywords: Active Defense; Electric Power Information Network Security; Intrusion Detection and Prevention System; Network Monitoring and Scanning; Threat Intelligence Sharing

Abstract: This paper delves into the critical applications of new active defense technologies in the security of electric power information networks. Through a comprehensive analysis of the threats and challenges faced by electric power information networks, it highlights the importance of active defense in enhancing the power system's resilience against complex threats. It details the fundamental principles and methods of active defense, including intrusion detection and prevention systems, abnormal traffic detection, and threat intelligence analysis. Tailored to the characteristics of the electric power industry, it also includes specific application cases such as network monitoring and scanning, threat intelligence sharing, behavioral analysis, and countermeasures. The paper summarizes the advantages and challenges of new active defense technologies and proposes future research directions, offering valuable insights for the continuous improvement of electric power information network security.

1. Introduction

With the rapid development of electric power information networks, the security and stability of power systems are increasingly under scrutiny. Facing continuously evolving network threats, such as attacks, breaches, and malware, traditional defense methods have become insufficient. Thus, researching and applying new active defense technologies has become a priority. This paper is dedicated to a thorough study of the application of new active defense technologies in electric power information network security, aiming to enhance the security and reliability of power systems.

2. Active Defense Principles and Methods in Power Information Network Security

In the current environment of power information network security, the application of active defense technology is crucial for the network security of power enterprises. Effective active defense principles and methods are central to protecting power systems from various network threats and attacks. The following discusses the fundamental principles and methods of active defense to ensure the robustness and reliability of power enterprise information networks.

2.1. Real-time Monitoring and Sensing

Real-time monitoring of network traffic, device status, and log records is a core principle of power information network security. This real-time monitoring mechanism allows the system to quickly detect any abnormal behavior, potential risks, or attack activities. Timely perception provides system administrators with crucial data support, enabling them to take necessary defensive measures immediately, ensuring the robustness and reliability of the power information network. In an evolving network threat environment, this active defense approach becomes an indispensable part of safeguarding power system security.

2.2. Threat Intelligence and Analysis

The integration of active defense technology with threat intelligence is an indispensable part of power information network security. By actively acquiring, integrating, and deeply analyzing the latest threat intelligence information, power enterprises can more comprehensively understand current threat trends, emerging attack technologies, and known attacker behavior patterns. This in-depth threat intelligence analysis allows enterprises to take preventive measures before attacks occur, effectively safeguarding against potential network threats and risks. The timely application of threat intelligence becomes a key strategy for power information network security, providing enterprises with more proactive network protection.

2.3. Intrusion Detection and Prevention Systems (IDS/IPS)

Intrusion Detection Systems (IDS) use specific detection rules, models, and algorithms to identify potential intrusive behaviors by analyzing network traffic, logs, and event data. Once a threat is identified, IDS can promptly alert and notify security administrators to take appropriate measures to ensure network security. This proactive intrusion detection mechanism acts as the first line of defense for power information network security, promptly detecting and isolating potential threats, helping to maintain the stability of the power system[1].

Not only can IDS detect intrusive behaviors, but Intrusion Prevention Systems (IPS) can take proactive measures to stop further attacks by intruders. For example, IPS can block malicious IP addresses, stop dangerous network connections, or reset connections, effectively curbing potential network threats. This proactive preventative approach enhances the overall defense capability of power information network security, ensuring that power enterprises can take timely and effective measures in the face of threats. The comprehensive application of intrusion detection and prevention systems builds a solid defense line for power information network security.

3. Advantages of New Active Defense Technologies

3.1. Early Attack Detection

New active defense technologies enable early detection of potential attack behaviors by real-time monitoring and analysis of network traffic and activities. These technologies can identify unusual data transfers, unauthorized access attempts, and malware propagation, and alert security administrators to take appropriate actions. This enables power companies to detect and prevent attack behaviors in a timely manner, reducing the risk of attacks. For example, Intrusion Detection Systems (IDS) in new active defense technologies continuously monitor the traffic and activities within the power information network. When IDS detects a large amount of outbound data traffic that does not align with normal business activities, it triggers an alarm and sends relevant information to the security administrator. The administrator can then take immediate actions, such as disconnecting the communication links with the attackers, to prevent further development of the attack.

3.2. Blocking Attack Exploitation Opportunities

New active defense technologies also help power companies to identify and remediate security vulnerabilities and weaknesses within the network. They can discover unpatched operating systems, open ports and services, and security configuration issues through vulnerability scanning and security configuration assessments. Timely remediation of these vulnerabilities and strengthening of the network can reduce the opportunities for attackers to exploit these vulnerabilities. For example, vulnerability scanning tools in new active defense technologies can conduct comprehensive scans of the power information network on a regular basis. The scan results reveal some unpatched operating systems and open ports. By promptly fixing these vulnerabilities, closing unnecessary ports, and strengthening password policies, the security of the power information network can be significantly enhanced, preventing attackers from exploiting vulnerabilities to gain unauthorized access.

3.3. Preventing Data Leakage

New active defense technologies also help power companies to prevent the risk of data leakage. They can monitor illegal data transfers and data leakage behaviors to detect and prevent the exposure of sensitive information early. For instance, data leakage monitoring systems in new active defense technologies can continuously track data transfer activities within the power information network. When the system detects that a computer suddenly transmits a large amount of data traffic, which is inconsistent with normal business activities, there might be a risk of data leakage. The system will promptly issue an alert and notify security administrators to take appropriate measures, such as disconnecting the computer from the network and resetting all connections on that computer, to prevent the leakage of sensitive information.

3.4. Understanding Threat Trends in Advance

New active defense technologies help power companies to stay informed about current threat trends and attack techniques, enabling them to devise appropriate defense strategies and measures. Through threat intelligence sharing, attack simulation, and security drills, power companies can obtain the latest threat intelligence from government agencies, security vendors, and third-party security service providers, learning about known threat behaviors, attack techniques, malicious software samples, and malicious IP addresses. Moreover, through attack simulations and security drills, power companies can understand the attack methods and tactics that attackers might use, and thus formulate targeted defensive measures. For example, power companies can share threat intelligence with other organizations in similar industries to stay updated on the latest attack trends and methods in the power industry. Additionally, power companies can also hire security consulting firms to conduct attack simulations and security drills to discover and remediate potential security vulnerabilities and enhance employees' security awareness and response capabilities.

4. Challenges of New Active Defense Technologies

4.1. Technical Complexity

Active defense technologies often require the use of advanced algorithms and complex techniques to implement functions such as network traffic monitoring and scanning, vulnerability remediation, and fortification. These technologies need to be configured and managed by professional technical personnel and may also require adjustments and optimizations to the network infrastructure. Therefore, technical complexity presents a significant challenge for new active defense technologies [2]. For example, real-time monitoring and scanning technologies involve large-scale data collection, storage, and analysis, requiring high-performance servers and powerful computing capabilities. Additionally, complex rules and models need to be established for anomaly detection and analysis, which demand higher feasibility and practicality from the technology.

4.2. Data Privacy Protection

Active defense technologies typically involve real-time monitoring and analysis of network traffic and activity data to detect abnormal behaviors and potential attacks. However, this process involves handling vast amounts of user data and private information, making effective data privacy protection a critical challenge. To address this, active defense technologies must comply with relevant privacy protection laws and regulations and adopt secure and reliable data encryption and anonymization techniques to protect user privacy. Moreover, establishing strict access control policies is necessary to ensure that only authorized personnel can access and use this data.

4.3. Compliance Requirements

Implementing new active defense technologies must consider compliance requirements. Different countries and regions may have various regulations regarding data privacy protection, security audits, and compliance, especially for power companies. Ensuring that active defense technologies comply with local laws, regulations, and industry standards is a significant challenge. To meet compliance requirements, power companies need to work closely with relevant government departments, regulatory bodies, and professional security service providers. By understanding and adhering to local laws and industry standards, developing appropriate security policies and measures, and conducting regular compliance audits and assessments, power companies can ensure the compliance of their active defense technologies.

4.4. Balancing Security Needs and User Experience

While enhancing network security, new active defense technologies must also consider user experience and convenience. On one hand, power companies need to strengthen network security to protect systems and data from attacks. On the other hand, users expect an efficient and convenient experience when using power services. When implementing new active defense technologies, power companies must balance the contradiction between security needs and user experience. For example, real-time monitoring and analysis of network traffic in monitoring and scanning technologies may impact network performance. Therefore, power companies need to adjust their monitoring strategies and frequency appropriately to ensure they can effectively detect potential attacks while maintaining a positive user experience.

5. Application and Advancements of New Active Defense Technologies in Power Information Networks

Network security remains a serious challenge for power companies, making the continuous development and application of active defense technologies particularly important. In power information networks, the adoption of new active defense measures can more effectively protect companies from various cyber threats and attacks.

5.1. Network Monitoring and Scanning

In the security framework of power information networks, network monitoring and scanning are considered foundational to active defense, playing a critical role as the first line of defense. By introducing advanced network monitoring technologies, power companies can monitor network traffic in real time, identify potential threats promptly, and take swift and robust protective measures, providing a solid guarantee for the stable operation of the power systems.

5.1.1. Application of Advanced Network Monitoring Technologies

Power companies are adopting advanced network monitoring technologies, such as Deep Packet Inspection (DPI) and traffic analysis, to fully understand network activity. These technologies allow for in-depth analysis of traffic at the packet level, identifying abnormal patterns and potential attack behaviors. Unlike traditional port scanning and simple signature detection, these advanced technologies can detect new threats more accurately, enhancing the sensitivity of network defenses.

5.1.2. Role and Frontier of Intelligent Power Devices

Intelligent power devices, as representatives of advanced technology in the security of power information networks, become powerful assistants in network monitoring and scanning through real-time sensing and monitoring. These devices can quickly identify abnormal traffic and respond in real time after detection, rapidly taking protective measures to minimize potential threats to the system.

5.1.3. Frontier Technology Trends: Artificial Intelligence and Machine Learning

With the ongoing development of technology, artificial intelligence (AI) and machine learning (ML) are gradually penetrating the field of network monitoring. These cutting-edge technologies can analyze massive amounts of network data and learn from it, automatically adjusting defense strategies based on the acquired knowledge. The introduction of intelligent algorithms will make power information networks more adaptive, accurately identifying unknown threats and further enhancing overall network security.

In power information networks, network monitoring and scanning are not only the foundation of active defense but also the first checkpoint for ensuring network security in power companies. By employing advanced network monitoring technologies and intelligent power devices, and introducing cutting-edge technologies such as AI and ML, power companies can more comprehensively and promptly detect and respond to potential network threats. This integrated network security strategy not only enhances the power systems' ability to withstand attacks but also maintains high vigilance in the ever-changing network security environment.

5.2. Threat Intelligence Sharing and Power Industry Cases

In building a strategy for power information network security, threat intelligence sharing is a crucial component. By establishing an inter-company power threat intelligence sharing platform, power companies can engage in information exchange with other businesses, gaining multi-source and multi-dimensional threat intelligence, thereby gaining a more comprehensive understanding of the threat landscape in the power industry and enhancing their ability to respond to new threats.

5.2.1. Threat Intelligence Sharing Mechanisms in the Power Industry

Power companies can establish a sharing mechanism that integrates their threat intelligence onto a cross-company platform. This mechanism not only aggregates security information from multiple parties within the industry but also achieves real-time updates, promptly reflecting the current threat situation. By sharing threat intelligence, companies can collectively address potential threats, forming a united front.

5.2.2. Typical Case: Successful Experiences in the Power Industry in Responding to Threats

Past cases in the power industry show that through threat intelligence sharing mechanisms, companies have achieved significant success in addressing various threats. For example, a power company learned about the transmission route of a new ransomware through the sharing platform and quickly implemented corresponding preventative measures, successfully avoiding potential attack risks. This case demonstrates the positive role of the sharing mechanism in enhancing the overall security level of companies.

5.2.3. Development Trends in Advanced Sharing Mechanisms

With the continuous development of artificial intelligence and big data technologies, the mechanism for sharing threat intelligence is also evolving towards more intelligent and real-time directions. In the future, automated threat intelligence analysis systems based on advanced algorithms will better serve power companies, achieving automated aggregation and dissemination of threat information. Such cutting-edge mechanisms not only increase response speeds but also more accurately identify and counteract potential threats.

In the context of power information network security, threat intelligence sharing is not only an active response strategy but also a crucial component in building a united security system within the power industry. Through the implementation of sharing platforms, power companies can leverage the wisdom and experience of multiple parties to collectively face evolving threats. As these sharing mechanisms continue to develop, power information network security is expected to embrace more intelligent and efficient protection methods.

5.3. Behavior Analysis, Countermeasures, and Power Industry Application Cases

In the security defenses of power information networks, behavior analysis and countermeasures are important means for power companies to guard against internal threats. By employing advanced behavior analysis technologies, power companies can identify and monitor normal and abnormal user behaviors, thus establishing a robust security barrier to reduce potential internal threats. This approach allows companies to preemptively address risks within their networks, enhancing overall security posture [3].

Behavior analysis technologies can differentiate between regular operational behaviors and activities that deviate from established patterns, which might indicate potential security risks or malicious intents. By continuously monitoring and analyzing user actions, power companies can quickly respond to any suspicious activities, implementing countermeasures to mitigate any potential damage.

For example, in a case within the power industry, behavior analysis helped detect an insider threat where an employee was attempting unauthorized access to sensitive system controls. The system flagged this unusual behavior based on the employee’s past activity records and current access levels. Immediate countermeasures, such as revoking the employee’s access privileges and conducting a detailed security audit, were effectively employed to prevent any actual breach.

This instance underlines the effectiveness of behavior analysis in protecting sensitive infrastructure and information. By integrating behavior analysis with comprehensive countermeasures, power companies can not only detect but also respond swiftly to internal threats, ensuring the integrity and reliability of their operations.

5.3.1. Development Trends in Advanced Sharing Mechanisms

As artificial intelligence and big data technologies continue to advance, the mechanism for threat intelligence sharing is also evolving towards more intelligent and real-time directions. In the future, automated threat intelligence analysis systems, based on advanced algorithms, will better serve power companies by automating the aggregation and dissemination of threat information. These cutting-edge mechanisms not only improve response speeds but also enhance the accuracy of identifying and countering potential threats.

In power information network security, threat intelligence sharing is not just an active response strategy but an essential part of building a united security system within the power industry. Through the implementation of sharing platforms, power companies can leverage collective intelligence and experience to confront evolving threats. As these sharing mechanisms continue to develop, power information network security will experience more intelligent and efficient protection methods.

5.4. Behavior Analysis, Countermeasures, and Power Industry Application Cases

In the security defenses of power information networks, behavior analysis and countermeasures are crucial for power companies to guard against internal threats. By employing advanced behavior analysis technologies, power companies can identify and monitor both normal and abnormal user behaviors, thus establishing a robust security barrier and reducing potential internal threats.

5.4.1. Advanced Behavior Analysis Technologies

Power companies can introduce advanced behavior analysis technologies to conduct real-time monitoring and analysis of employee activities within the power information network. These technologies utilize machine learning and pattern recognition to establish baseline models of employee behavior and can quickly detect activities that deviate from normal behavior patterns.

5.4.2. Application of Behavior Analysis in Power Companies

For example, in power systems, behavior analysis can monitor employee access behaviors to promptly detect unauthorized access or abnormal operations. This real-time feedback enables companies to take preventive measures before threats materialize, securing the overall safety of the power information network.

5.4.3. Case Display: A Power Company's Success Story

A leading power company implemented an advanced behavior analysis system and successfully identified an internal employee illegally accessing the power system. Thanks to the real-time alert system, the company could quickly respond, isolate potential risks, and strengthen control over internal access permissions [4]. This successful case highlights the practical effectiveness of behavior analysis in power companies, not only significantly reducing the potential risks posed by internal threats but also injecting new confidence into the security of power systems. The successful application of these proactive defense measures provides a reference for other power companies and underscores the critical role of behavior analysis in enhancing the security level of power information networks.

5.5. Rise of Artificial Intelligence Technology

Power information network security will increasingly rely on artificial intelligence technology. Through machine learning and deep learning, systems can perform real-time analysis of large-scale data, accurately identifying new threats and responding swiftly. In the future, power companies will utilize smart technologies to automate network defense, enhancing both response speed and precision.

5.5.1. Widespread Application of Blockchain Technology

Blockchain-based power information network security will become key to preventing data tampering and malicious attacks. The decentralized and immutable nature of blockchain ensures the integrity and trustworthiness of power information. In the future, power companies can use blockchain to establish a distributed security framework, enhancing data security and ensuring uninterrupted operation of power systems.

5.5.2. Integration of Smart Networks and Proactive Defense

The future trend will be the deep integration of smart networks with proactive defense. Power companies will work with intelligent network structures in tandem with proactive defense technologies to achieve comprehensive monitoring and protection of networks. This integration will make power information networks more resilient, better adapting to rapidly changing network threats.

Power information network security is entering a new era led by intelligent technologies and blockchain. Artificial intelligence will enhance the automation of network defenses, while blockchain-based security measures will strengthen data protection. The deep integration of smart networks with proactive defense will build a more secure and reliable information network for power companies, ensuring stable operation of power systems without disruption from threats. Power companies should actively keep up with these advanced technologies, continually upgrading their network security strategies to adapt to the evolving threat landscape[5].

6. Conclusion

The introduction of new proactive defense technologies brings new possibilities and challenges to power information network security. By deeply exploring their applications in the power sector, we find that these technologies effectively enhance the network's ability to handle complex and intelligent threats, thereby improving network security and stability. However, we must also recognize that new proactive defense technologies face a series of challenges, including technological complexity, data privacy protection, and compliance issues. Future research should aim to address these issues to improve the feasibility and practicality of proactive defense technologies, advancing the ongoing development of power information network security. Through relentless efforts, we can hope to build more robust and intelligent power information networks, ensuring they can respond more calmly and efficiently to future threats.

References

[1] Zhou Liang. New Proactive Defense Technologies and Their Application in Power Information Network Security. Electronic Testing, 2021(06):119-120.

[2] Niu Fei. Analysis of New Proactive Defense Technologies and Their Application in Power Information Network Security. China Communications, 2018, 20(21):124.

[3] Wu Ying, Wang Lei. Exploration of the Application of New Proactive Defense Technologies in Power Information Network Security. China Communications, 2018, 20(17):131.

[4] Zhong Ye. Application of New Proactive Defense Technologies in Power Information Network Security. Electronics Technology and Software Engineering, 2017(24):209-210.

[5] Xu Zhigang. Research on Security Architecture and Proactive Defense Technologies in Enterprise Cloud Computing Data Centers. Nanjing University of Posts and Telecommunications, 2021.