Research on Power Enterprise Network Security Solution

Shang YanWei¹, Lin Qiang¹, FengZhi Peng¹*
¹Guangdong Power Grid Co., Ltd IT Information Center, Guangdong, 510030, China

Abstract: With the development of scientific and technological productivity, the operation and maintenance of power companies have gradually realized network informationization. However, there are still some risks in the computer network security of power companies. The article first expounds the importance of computer network security and then analyzes the risks existing in the power system computing network and finally puts forward targeted computer network security protection measures.

1. INTRODUCTION
With the advent of the information age, computer networks are increasingly used in power enterprises and they can achieve integrated management in power system automation, monitoring, protection and collection of electricity charges, playing an increasingly important role. At the same time, the national power data communication network also connects various levels of power companies to achieve information sharing. However, due to various factors, the security risks of power enterprise information networks are increasing, network data is lost, operating systems are destroyed and network failures occur from time to time. The safe and reliable operation of power companies is the basic guarantee for ensuring the normal operation of social production and life. How to ensure the computer network security of power companies is an important issue to be solved urgently in the power industry. Based on this, the author discusses this issue[1].

2. THE IMPORTANCE OF COMPUTER NETWORK SECURITY
Computer network security mainly includes two aspects: information security and physical security. Information security refers to network security to ensure the integrity and confidentiality of various network data information. The threat sources of computer networks include viruses, hackers, etc., in which the harm caused by hacking attacks has exceeded the impact of viruses and some attacks are even fatal. Therefore, it is necessary to strengthen the security of computer networks. Only by taking targeted protection measures can we ensure the security and integrity of network information. According to the US Federal Survey, the annual economic losses caused by computer network security in the United States amount to 27 billion yuan per year. The security threat of the domestic Internet is also very serious. According to the 2013 National Emergency Assessment Center's assessment data, 58% of the global "zombie" computers are in China. It can be seen that ensuring the security of computer networks is imperative[2].

3. RISKS OF COMPUTER NETWORKS IN POWER COMPANIES

3.1. TECHNICAL SECURITY RISKS
With the advent of the information age, the dependence of power companies on computer networks has reached an unprecedented scale. Due to the huge security risks of computer networks, the security
and stability of power system operations that are over-reliant on computer networks become very fragile. Once the computer network is damaged due to various reasons, the entire power system will be paralyzed. Based on this, power companies must develop comprehensive computer network security protection measures to ensure the safe and stable operation of the power system. However, the current security protection technology has certain pertinence. It is usually designed separately for one or several problems. It is difficult to effectively solve all the problems that arise during operation and it is difficult to provide comprehensive security protection for computer network security. There are certain deficiencies in technology[3]. The frequency of occurrence of various risks is shown in Table 1.

| Years | Technical | Information | Managing |
|-------|-----------|-------------|----------|
| 2011  | 511479    | 42847       | 634840   |
| 2012  | 532098    | 44560       | 654562   |
| 2013  | 552717    | 46273       | 674284   |
| 2014  | 573336    | 47986       | 694006   |
| 2015  | 593955    | 49699       | 713728   |
| 2016  | 614574    | 51412       | 733450   |
| 2017  | 635193    | 53125       | 753172   |
| 2018  | 655812    | 54838       | 772894   |
| 2019  | 676431    | 56551       | 792616   |
| 2020  | 697050    | 58264       | 812338   |
| 2021  | 717669    | 59977       | 832060   |

3.2. INFORMATION SECURITY RISK
At present, the reasons for threatening the security of computer networks in power systems include: natural disasters, software vulnerabilities, viruses and hackers. Computer systems are easily affected by natural disasters such as fires, lightning strikes, earthquakes, etc. Once such natural disasters occur, if the protection capacity is insufficient, it is easy to cause loss of power system information. Due to the variety of application network software and different types of vulnerabilities, hackers exploit software vulnerabilities to attack software and ultimately destroy the entire system. Viruses also have an impact on computer network security. Once the network interferes with the virus, it may cause the entire system to run slowly, which may lead to system loss and data loss. In addition, some lawless elements have deliberately destroyed power system data and implemented financial crimes by stealing passwords, etc., which have greatly threatened computer network security[4].

3.3. MANAGING SECURITY RISKS
Management security risks mainly exist in two aspects: first, network management personnel; second, network users. Managers and users are not aware of security. They can use their own accounts or share them with others. They use pirated applications and externally insecure mobile storage media to inadvertently reveal key information such as network passwords and configurations. Problems can easily affect the safe and stable operation of the network.

4. POWER ENTERPRISE COMPUTER NETWORK SECURITY PRECAUTIONS

4.1. USING SWITCHES AND VIRTUAL LAN TECHNOLOGY TO ACHIEVE ACCESS CONTROL
In order to improve the security of the computer network of the power enterprise, the switch and the virtual local area network technology can be adopted to divide the power enterprise into multiple subnets according to different service types and security requirements and the firewall is used to effectively isolate the internal and external networks. For example, the power enterprise's database, email, etc. can be divided into one VLAN1 and the power enterprise external network is divided into
another VLAN2. At the same time, the one-way information flow between the two can be controlled, the former can access the latter and the latter cannot visit the former. In order to ensure the security of the management, the nodes of the unified department of the power enterprise can be divided into the same virtual network and different management rights are assigned to different management personnel. The three-layer switch is used to support the configuration access rights of the unified network. It can effectively isolate broadcast storms and can also complete route routing and reduce delay. Specifically, several measures can be taken: first, control the MAC address port; second, use IP packets for filtering at the network layer; third, register the MAC addresses of all user machines of the power system to ensure that only authorized users can enter[5].

4.2. INFORMATION ENCRYPTION TRANSMISSION

Power enterprise information is vulnerable to hackers in the transmission process. Routers and switches of computer networks are easily attacked by hackers. Based on this, in order to prevent data information from being eavesdropped, modified and leaked during transmission, etc. The transmitted data can be encrypted so that it can be transmitted and stored in ciphertext. For the security networking requirements of different data information of the power system, the data transmission can be realized through different network layers. If the data information is transmitted at the physical layer, link encryption can be used, that is, a corresponding encryption device is installed at each communication link port. For example, in the network and transport layer, when the packet enters the packet switch, the related information must be decrypted so that the route of the link can be correctly determined. In this decryption process, the data is also vulnerable to attacks, based on which the network can be transmitted. The layer implements end-to-end encryption to ensure security during the decryption of information. Information encryption algorithm such as formula 1.

\[ E(W, B) = \frac{1}{2} \sum_{k=1}^{2} (t_k - y2_k)^2 \]  

(1)

4.3. DIGITAL SIGNATURE AND IDENTITY AUTHENTICATION

In the network operating environment, the system and the system, the system and the user, the user, etc. continuously and frequently carry out the information transmission process, it is easy to exist several security risks: First, there is a fake source point identity will be the message Insert into the network; second, confirm or not accept the fake; third, tamper with the content and serial number of the message. In this case, the most effective solution is to authenticate the data modification personnel. The digital signature and certificate technology can be used to ensure the authenticity and validity of the user and the identity of the distributor can be recognized. The receiving aspect can also pass the number. Signatures and other methods to determine whether the data is derived from the integrity of the specified user and data information. In addition, digital signatures can also effectively prevent the negative problem of transmission in this article.

4.4. POWER ENTERPRISE EXTERNAL NETWORK SECURITY ACCESS CONTROL

Power companies use the Internet to achieve effective connections and access to the outside world. In order to ensure the security of information access and transmission in this process, firewall technology is usually adopted. Between the internal and external networks of the power enterprise, the firewall is used to achieve isolation and access control; the access control of different network security domains within the power enterprise also uses a firewall, so as to effectively isolate access control between different networks and avoid a network problem affects another network segment through the local area network. Through this setting, real-time detection and audit of network activities, events and status can be realized and real-time analysis and control of various malicious access control and misoperations can be performed; relevant analysis reports can be obtained according to firewall monitoring and vulnerability detection. According to the content of the report, the power system users are provided with rapid detection of illegal intrusion and provide counterattack means. Therefore,
setting the firewall correctly can not only effectively realize the security protection between the internal and external networks, but also provide security protection between different internal network segments and effectively reduce the network security risk of the power system according to the needs of users.

4.5. LOG MANAGEMENT AND BACKUP DATA

For the power system, in addition to the above-mentioned security protection, the log management and backup data subsystem are the key to ensuring the security of information data. If these two systems are lacking, it is difficult to put into actual operation, so the power system computer network appears. Failure, must first analyze the cause of the problem and can restore the normal operation of the system in the shortest time, that is, the key link of the network system design, log management is mainly to record the operation into the power system, such as database operations, FTP File server, etc. The operation events mainly include: clicking the menu item, clicking the window control, button, drop-down box, etc.; the log table record mainly includes: user name, login time, location, exit time, operation content, etc., so as to be used in future auditing and verification. The power enterprise data is the life of the enterprise. Once the data is lost, the losses caused to the enterprise are immeasurable. To prevent data loss or damage, the database must be archived and backed up in time. Archiving refers to the permanent or restricted saving practice of saving data that is not needed by the database. Data backup is the most basic daily work of the power system. When building a computer network system, you must first set the backup time, backup data selection, etc. to ensure the security of data information.

5. CONCLUSION

The computer network security of power companies belongs to a complex system engineering, involving advanced security technologies, perfect system management and many other aspects. In order to ensure the safe operation of computer network systems, a multi-level and comprehensive security system must be established. This paper carefully analyzes the security requirements of power companies for computer networks and carefully studies the security, efficiency and convenience of power companies and comprehensively utilizes data encryption, firewalls and virus detection to ensure the security of computer networks.

References

[1] Sebastian Feyrock. Łukasz Kulesa: Envisioning a Russia-NATO Conflict. Implications for Deterrence Stability. London: European Leadership Network (Euro-Atlantic Security Report), Februa 2018[J]. SIRIUS - Zeitschrift für strategische Analysen,2018,2(3).
[2] University of Michigan; Patent Issued for Rating Network Security Posture And Comparing Network Maliciousness (USPTO 10,038,703)[J]. Computers, Networks &amp; Communications,2018.
[3] José De Sousa,Daniel Mirza,Thierry Verdier. Terror networks and trade: Does the neighbor hurt?[J]. European Economic Review,2018,107.
[4] Tahir Hasan,Tahir Ruhma,McDonald-Maier Klaus. On the security of consumer wearable devices in the Internet of Things.[J]. PloS one,2018,13(4).
[5] Sergei Shubin,Maria Nesterenko. The Arctic: network diplomacy from the view of global security 2.0[J]. The Polar Journal,2018,8(1).