# Problems and countermeasures in the management of network security in the rural grassroots sector

*Hua Lu*
Net Information Office of Dongtai Municipal Party Committee, Jiangsu dongtai,postcode: 224200

**Abstract:** On 15 August 2017, the General Office of the Central Committee of the Communist Party of China (CPC) issued the Implementation Measures for the System of Responsibility for Network Security Work of Party Committees (Party Groups), marking the formal establishment of China's network security responsibility system. In recent years, local party committees (party groups) at all levels have attached great importance to the work of cyber security, with initiatives, innovations and results. However, there are still problems in the rural grassroots sector such as insufficient attention, inadequate funding and weak technical capacity, which have constrained the level of rural government services and high-quality rural development.

**Keywords:** rural grassroots sector; cybersecurity issues; countermeasures

In recent years, the pace of information construction of government systems and office systems has been accelerating, especially the information systems of some vertical departments, which cover a wide and powerful area from top to bottom, greatly improving the quality and efficiency of all kinds of government management. However, for various reasons, there are many problems in network operation and maintenance, especially in the operation and maintenance of grass-roots systems or terminals, which seriously affect the security of information systems and the reliability of data.

## I. Problems

1. Weak awareness of security precautions. During our work, we found that many grassroots cadres believe that there are specialized technical personnel on the intranet, and that the security issues of the system terminals developed by the superiors are naturally the responsibility of the superior departments. Moreover, firewalls and anti-virus software have been installed, so there should be no more problems, and even if there are problems, it has nothing to do with the operators. There is also a lack of professional and technical personnel in some grassroots departments. They do not set up full-time network security management positions, or one person uses multiple posts and part-time jobs. It is impossible to devote all their energy to network security prevention and monitoring. If part of the time is taken up by other work, it is more likely that you will not be able to participate in various business trainings, and you will lack the reserve and update of relevant knowledge. Specifically reflected in several aspects: First, do not set a password or set a weak password. For the sake of simplification of work, the terminal operator cancels the password input link, or directly uses the system initial password, or multiple people share the same password to prevent forgetting, or sets a simple password that everyone knows, such as "123456" and "000000"; The second is that the anti-virus software is not installed in time. Regarding the software installation work, under normal circumstances, when the unit installs the office system, the technicians will simultaneously install the anti-virus software. Therefore, most of this kind of situation out of software late updates and patches, the vast majority of staff will be under the illusion that they will not need to update after one installation, so that the vulnerability into the entrance to the virus. Thirdly, setting up sharing is too random. The work found that the same type of office personnel, or the same system personnel, often need to call or read the same type of file, compared to U disk, CD-ROM or mailbox and other means of transmission, set up a shared directory is easier and faster, different terminals to access the shared file itself has been a security risk, coupled with the use of shared without timely cancellation of settings, in the long run, is bound to threaten the security of the system; fourth is mixed use of internal and external networks. With the continuous improvement of some systems and data security level, the grassroots units also gradually put forward the requirements of the internal and external networks to use separate machines, to take physical isolation means, confidential information by a dedicated person dedicated machine disconnected from the network, but a very small number of people have a fluke mentality, that once or twice will not be a problem, the transmission of confidential information on the external network, or the internal network machine online use, etc..

2. hardware maintenance management is not in place. Due to funding, attention and other reasons, the more we go to the grassroots level, the more the problems of inadequate configuration and poor management of hardware are highlighted, especially in some units with tight office funding, computer peripherals and other equipment aging, not updated in a timely manner is very common, such as uninterruptible power supply used for too long, too little memory, insufficient hard disk space, etc., often causing the computer to crash or restart, affecting the progress of government systems. In particular, some window units, due to computer failure led to a lengthy office process, triggering public dissatisfaction; in addition, because of the lack of awareness of prevention at the grassroots level in rural areas, generally not installed lightning protection facilities, coupled with most rural lines simple and old, once the event of a lightning strike, transmission node damage, will inevitably occur the destruction of network equipment, resulting in the loss of key data and other negative impacts of varying degrees.

3. operator follow-up management is not perfect. As mentioned earlier, the grassroots units generally have no full-time technical staff, frequent staff turnover and other problems. Therefore, each unit is basically no longer responsible, and the work of network access, use, and maintenance has been packaged to major network service providers. Operators often only show up when there is a network failure in the

unit, and it is impossible to provide daily network maintenance to grassroots units. The network information department where the author works organizes an investigation of the Internet assets in the area every year, and strives to discover hidden dangers in network security in a timely manner and supervise and rectify them. However, during work, it was discovered that the grassroots units were not clear about the concept of "Internet assets", and they were unable to correctly report which assets belonged to the Internet in their units, so they had to turn to local operators for help. However, because routine maintenance is not carried out, often the technicians of the operator cannot clearly explain the asset status of the unit, thus falling into an embarrassing situation of no one to manage, and it is impossible to solve the faults and problems in the shortest time.

## II. Causes of the problem

1. The problem of subjective consciousness. Consciousness determines thinking, thinking determines behavior, behavior determines the consequences. It is precisely because the grassroots units do not pay attention to it ideologically that a series of problems have arisen, such as: the level of network security management is not high, the management system and mechanism are not perfect, no effective emergency plan has been formulated, and network security incident drills have never been conducted. As a result, the ability to prevent and prevent network attacks is seriously lagging behind, and there is nothing to do after a network security incident occurs. At the same time, the construction of personnel echelons in grassroots units is not in place. The general age structure from unit leaders to staff members is too large. There is no concept of setting passwords, daily virus removal, physical isolation, security warnings, etc., which is also one of the reasons for the formation of hidden dangers in network security.

2. Objective development issues. With the rapid development of the Internet, the use of new technologies such as 5G, artificial intelligence, biometrics and the Internet of Things, the boundary between the network world and the real world is becoming increasingly blurred, and massive amounts of data are circulated and shared frequently. As we all know, no matter how advanced the system, how smart the equipment, how complete the application, the first element is people. Whether it is computer software, hardware or network systems, they are all programmed by people. Since people are the main cause, it is inevitable that there are loopholes and defects, which provides "opportunities" for viruses and hackers to attack the network. If there is a "mole" involved, with some ulterior motive, then any minor oversight on our part will expose the network security of the entire system.

## III. Countermeasures

1. the ideological importance. From the ideological point of view, it must be highly valued. This is definitely not an official phrase. Only when everyone pays attention to network security issues and conscientiously implement the party committee (party group) responsibility system for network security work can we provide full-time and all-round supervision and protection in terms of systems, mechanisms, technologies, and actions, and ensure the safe operation of the network system as much as possible. Many comrades in the grassroots units may have a fluke mentality, or the idea that it has nothing to do with themselves, thinking that a few operations that are not rigorous will not cause serious consequences. Even if a network security problem occurs, it is only a problem with the unit system and data, and will not affect individuals. But "no snowflake is innocent during an avalanche, and no snowflake can stay out of it." In front of the Internet, we are all transparent people. Usually online shopping, chatting, sending and receiving emails, and various APPs will expose personal information. A large amount of information such as name, ID number, phone number, address, hobbies, etc. is combined into every different individual on the network. Once a network security incident occurs, a large number of individuals Information leakage must affect each of us.

2. Increase investment. The main person in charge of the grassroots unit must pay sufficient attention to the network security management work. Increase the investment in special funds for network security maintenance, keep pace with the times to solve the update frequency of computer hardware facilities, purchase genuine anti-virus software and upgrade it in place daily, increase cooperation with third-party network security protection units, and introduce advanced professional technology talent. According to the unified deployment requirements of the central government, provinces, and municipalities, the domestic equipment replacement plan is compiled and reported in a timely manner and updated in strict accordance with the schedule and progress, so as to ensure that the replacement and technical support of various network equipment and security protection equipment will not be affected. It is necessary to ensure that security protection funds are in place, and that security technology protection is in place, so as to prevent network security from being in a state of passive blocking and response, form an overall awareness of active defense and active response, and fundamentally improve the unit's network protection, monitoring, response, fight and recovery capabilities.

3. Sound mechanism. There are rules to follow in everything, someone is responsible, someone supervises, and there is evidence to check, so as to ensure that the network security management work is implemented. First of all, there are rules to follow, not only to establish rules and regulations, but also to pay attention to follow-up assessment and rewards and punishments. Which behaviors are prohibited, which behaviors should be praised or even promoted, must be clarified one by one and the results reported. Secondly, the truth of "the three monks have no water to drink" is simple and easy to understand. There must be a clear division of labor in the special work of network security, and a special person should be designated to be responsible, so as to effectively shoulder the responsibility and avoid the phenomenon of mutual shirk. Third, no matter how clear the system is, no matter how comprehensive the meetings are arranged, it will not be as good as the follow-up supervision and assessment. To strengthen the result orientation, the unit can adopt a combination of full-time supervision and public evaluation to evaluate the network security work. The network security supervision department combines regular and irregular periods to sort out and supervise the Internet usage of each unit. Finally, "well-documented" forms a closed loop of network security management,

highlighting the importance and necessity of inspection and supervision. Whether the technicians are dedicated, whether the results are in place, etc., passed the inspection, and also conveyed to everyone the concept of "network security work is extremely important".

4. Upgrade your skills. Be prepared in case of danger. A period of network security does not represent the eternal security, the security of a system does not represent the security of the entire network, only the usual prevention of danger in advance, in order to try to avoid the occurrence of danger, even if the danger occurred, can also try to turn it into safe. To combine the actual work of the unit, develop a practical network security emergency response plan to improve the ability to respond to network security incidents, prevent and reduce the damage and harm caused by network security incidents, protect the public interest and maintain national security, public safety and social order. Including equipment damage, operational errors, hacker attacks, etc., regular practical exercises, for network security incidents, according to the severity of the event, the scope of impact and the degree of harm, adhere to unified leadership, hierarchical responsibility, rapid response, scientific disposal, do a good job of daily backup of key data in key areas, organise skills training for professional and technical personnel at the grassroots level, give full play to the strength of all parties to do a good job together prevention and disposal of network security incidents.

## References

[1]Liu Bicheng. Research on the Problems and Countermeasu res of Chinese Government Information Security Managen ment System[D]. Jilin University, 2021.

[2]Cai Wenhao. Refined management of information security service project process[D]. Donghua University, 2022.

[3]Li Deming. Research on Network Information Security Supe ervision System in China and The Relationship between Subjects[D]. Beijing Jiaotong University, 2020.

[4]Zhou Yusuo. Discussion on Influencing Factors and Preventive Measures of Computer Network Security Technology[J]. Network Security Technology & Application, 2023.

**Contact:** Lu Hua, Net Information Office of Dongtai Municipal Party Committee, Jiangsu Province.