THE NEW REQUIREMENTS OF INFORMATION SECURITY PROTECTION ON STATE GRID SHANGHAI MUNICIPAL ELECTRIC POWER COMPANY DATA CENTER COMPARED TO DISASTER RECOVERY CENTER

HU Junyi
State Grid Shanghai Municipal Electric Power Company – China
hhhy2j_hu@hotmail.com

LU Rong
State Grid Shanghai Municipal Electric Power Company – China
vivirong1122@hotmail.com

ABSTRACT

According to State Grid's unified planning, State Grid Shanghai Municipal Electric Power Company DISASTER RECOVERY will be transformed to DATA CENTER.
In this paper, according to the practical situation of transforming Shanghai Municipal Electric Power Company DISASTER RECOVERY CENTER to DATA CENTER, the principal of information security protection was studied, and the new requirements of information security protection on DATA CENTER were described.

INTRODUCTION

Along with tight combination of information technology (IT) and power system, data reliability and business continuity of information system becomes more and more important for power grid enterprises. According to State Grid's unified planning, State Grid Shanghai Municipal Electric Power Company DISASTER RECOVERY will be transformed to DATA CENTER, gradually changing deployment of application information system from decentralized deployment (used now) to centralized deployment in DATE CENTER for unified management and monitoring, it can realize quicker response to business, more efficient coordination and more reliable service for State Grid Company, also it is an important component of Smart Grid construction.
In contrast to DISASTER RECOVERY CENTER, it makes information security issues more crucial under operation mode of DATA CENTER. According to the practical situation, the following 4 points of new requirements of information security protection should be studied and applied.

AREAS AND DOMAINS SEPARATED

In condition of DATA CENTER, because of deployment of information systems such as e-commerce, marketing, electric energy remote collection system etc, the network border of DATA CENTER increased, including Internet and Wireless Network.
According to the importance of different application information system and data sensitivity, each application information system was required to be distinguished for a certain security level. Different physical areas and logical domains were separated to deploy systems based on security level and access path in DATA CENTER, shown as Fig1.

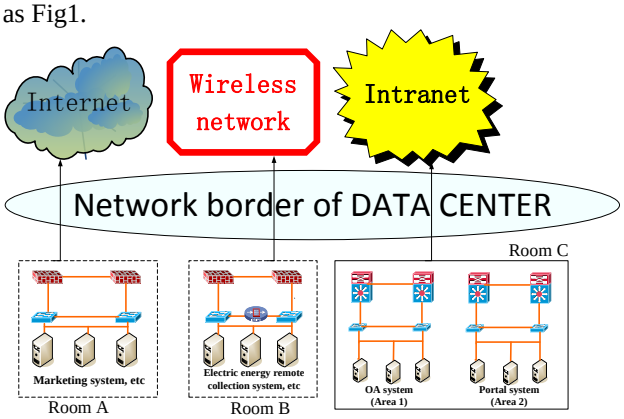

Fig1 schematic diagram of physical areas and logical domains of Shanghai Municipal Electric Power Company DATA CENTER

NETWORK FLOW MANAGEMENT

During business peak period, large numbers of users connecting to application systems may cause explosion of concurrent sessions and network flow. New methods and principles were required to control and arrange the network flow of every application system reasonably. It was required to guarantee no network congestion, business continuity and good user experience.
To solve this problem, monitoring agents will be deployed at every border of network by planning in order to make instantaneous analysis of network flow. In case the business of a certain application system surging at one moment, dynamic control of the flow of other systems would be applied. The control strategy should be kept to such principle, network flow of disaster recovery systems decreasing firstly, then flow of level-2 application system decreasing, flow of level-3 application system controlling at last.

HIGHER AUTHENTICATION FOR STORAGE

Now, in Shanghai Municipal Electric Power Company DATA CENTER, high-class shared disk array was used for system storage. It means multiple application systems were attached to one high-class shared disk array. Thus, a higher level authentication method was required to substitute for WWN authentication method used now. It

includes storage encryption, data access control, ID authentication, IO management and etc, shown as Fig2.

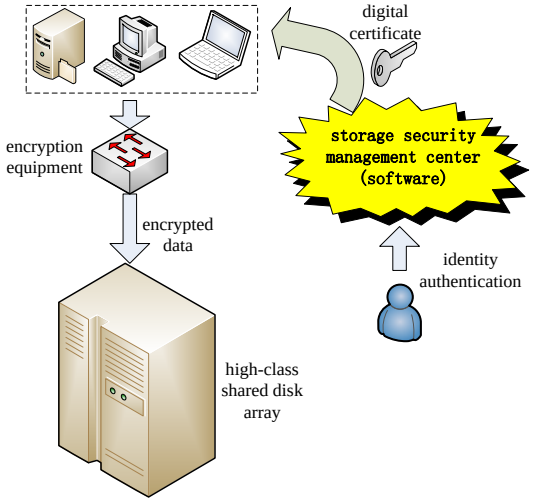

Fig2 storage management system under operation mode of DATA CENTER

Data encryption technology

In DATA CENTER, these two kinds of data (business data and mirror image files of virtual machine) are assessed to be protected necessarily by using encryption methods. Besides, the border of encryption should be as close as to the position where the data generated. The nodes that generate date in DATA CENTER are application servers, therefore, encryption equipment should be deployed at the exit of application servers. So, the data would be already encrypted as soon as get rid of users' supervision to prevent the probability of security problems such as unauthorized access to business data, malicious migration of virtual machines by system administrator and etc.

Data access control

In SAN (Storage Area Network) network, authentication software will be installed on the application servers. Under strong authentication mode, the authority will be strictly limited for accessing logical storage unit by application servers. Meanwhile, by binding the identity of application servers with LUN (Logical Unit Number), data access base on disk level will also be strengthened to ensure the identity security of servers.

ID authentication and IO management

Storage security management center will be established to make necessary verification of settings and identification. The access will be interrupted immediately from IO level of equipment if any violation or illegal occasion occurs.

SECURITY ON VIRTUAL MACHINES

Application of virtualization technology becomes more and more wildly applied in application systems. The boundary of system turned to boards or ports instead of equipment itself. Therefore, more precise security protection strategy was required as follows.

NIC (Network Interface Card) bonding

All physical servers will be required to install at least 2 NIC and finish bonding. So if any NIC or network cable malfunctioned, the virtual machine that was deployed on the physical server would provide continuous service.

Setting up private VLAN (Virtual Local Area Network)

The ports that have business related association will be set up to a private VLAN, which is similar to the VLANs on the switches, but precisely refined to a certain port of a physical server.

vCenter security configuration enabled

On virtual machine level, user authorization management, identity authentication, hot standby function, etc will be redefined according to the practical operation situation of virtual machines.

CONCLUSION

Although the 4 points of new requirements of information security protection mentioned above could meet the recent needs of DATA CENTER, the principle and requirements of information security protection should always be studied and improved to make DATA CENTER (DISASTER RECOVERY CENTER) be an important information support for Smart Grid construction.