电信行业网络信息安全体系的建设

Network Information Security System Building for Telecommunication Industry

周振宇 （华中科技大学电子与信息工程系）

摘要：针对电信运营商提出了IP网络安全体系结构，并给出安全体系的部署步骤

关键词：信息网络安全　信息安全管理体系

1 信息安全体系

1.1 信息安全的概念

信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。信息安全是指信息系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

从广义来说，凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术及理论都是信息安全的研究领域。广义的信息系统安全的范围很广，它不仅包括信息系统本身，还包括自然灾害（如雷电、地震、火灾等），物理损坏（如硬盘损坏、设备使用寿命到期等），设备故障（如停电、电磁干扰等），意外事故等。狭义的系统安全包括计算机主机系统和网络系统上的主机、网络设备和某些终端设备的安全问题，主要针对对这些系统的攻击、侦听、欺骗等非法手段的防护。

1.2 安全体系结构

电信运营商的数据业务通常既提供用户的接入业务，又提供各种应用服务，因此必须建立一个完善的安全矩阵来保护其网络、应用业务系统。

一个完整的安全矩阵，主要从物理环境、网络、主机与应用和安全管理体系四个方面进行部署。物理环境安全主要指的是机房、设备环境安全。网络安全主要包括用户接入、通信链路和网络设备的安全。主机与应用安全主要指主机系统、数据库系统和应用系统的安全。安全管理体系主要指形成一套完整的IP网络系统安全解决方案所必须配备的管理制度，它是实现信息安全的落实手段。如图1所示。

(1) 用户接入层安全

用户接入安全指保障合法用户的正常接入（登录），阻止非法用户的网络接入（登录），保障接入系统的设备、软件、数据等的安全。用户一旦接入，其身份应具有非伪装性，其行为具有不可抵赖性。

(2) 网络安全

网络安全是指网络系统中的通信链路、路由器、交换机等设备和数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，保证系统连续可靠正常地运行，网络不中断。网络安全应具备：控制不同的访问者对网络和设备的访问权限；划分并隔离不同安全域；防止内部访问者对无权访问区域的访问和误操作；能够预防、制止各种网络攻击，如路由攻击、SNMP攻击、路由器和消耗带宽攻击、Telnet攻击等。

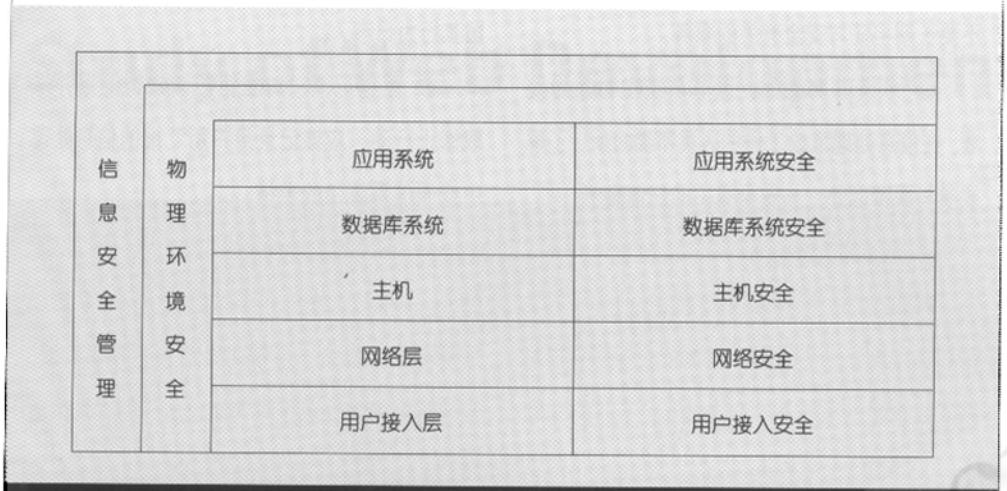

图1 安全体系结构

(3) 主机安全

主机安全指主机操作系统、系统软件和系统重要数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，保证系统连续可靠正常地运行，服务不中断。主要包括：主机设备安全，操作系统安全，文件系统安全，用户帐号、权限安全，用户登录、权限控制，缓冲区溢出，拒绝服务攻击（DoS、DDoS等），特洛伊木马，网络监听，电子欺骗（包括硬件欺骗、ARP欺骗、路由欺骗、TCP连接欺骗等），计算机病毒等。

(4) 数据库安全

数据库安全是指数据库系统软件和数据受到保护，软件系统不受非法攻击和窜改，数据不受非法访问、修改、删除，保证系统连续可靠正常地运行，服务不中断。主要包括：数据库软件系统安全，用户帐户安全，用户权限安全，数据安全，缓冲区溢出，拒绝访问攻击，木马等。

(5) 应用系统安全

应用系统安全指保障应用软件、数据等的安全，使其不受非法的访问、修改、删除等，应用系统连续、高效、可靠、正常地运行，应用不中断。由于应用软件的设计管理是与其运营模式分不开的，同时也是建立在网络、主机和数据库系统基础之上的，因此业务部分的软件分发、用户管理、权限管理需要充分利用底层系统的安全技术和良好的安全管理机制。主要涉及的应用有：各种因特网服务（如DNS、邮件、WEB服务、FTP服务等），增值数据业务，网管、计费系统，综合营帐系统等。

(6) 物理环境安全

物理环境安全指机房、硬件环境的安全。包括机房的温度、湿度、气压，防火、防雷、防震，电力供应，机房布线等。

(7) 安全管理

在安全体系中，最为重要的是安全管理。它包括确定全网的安全方针策略，建立行之有效的安全组织机构和安全制度，配备专门的安全人员、明确安全职责，对人员不断地进行安全教育和培训等。

2 安全体系的部署

要进行安全体系的部署，首先要找出影响信息安全的问题。这些问题主要集中在两个方面：一是技术因素，系统本身存在的安全脆弱性；二是管理因素，组织内部的信息安全管理制度不完善。即计算机网络与信息安全=信息安全技术+信息安全管理体系（Information Security Management System，ISMS）。技术层面和管理层面的良好配合，是实现网络与信息安全系统的有效途径。其中，信息安全的技术层面通过采用包括建设安全的网络系统、安全的主机与应用系统，并配备适当的安全产品、获取安全服务的方法来实现；在管理层面，则通过构架信息安全管理体系来实现。

2.1 安全产品的部署

安全产品对安全事件的处理一般分为事前、事中与事后的处理。

事前对网络信息系统进行安全评估，对各种已知安全漏洞进行扫描，提供安全评估结果，并对安全漏洞进行修补或提出有效的建议。此类产品和服务主要有网络漏洞扫描、主机漏洞扫描、数据库漏洞扫描，安全评估服务，访问控制等。

事中处理是指监视用户及系统的活动，统计并分析异常行为模式，审计跟踪管理操作系统，识别违反安全策略的操作，保护重要数据的安全性，识别正在进行的攻击活动，对影响系统安全的行为及时作出响应，比如切断连接、记录事件和报警等。此类产品主要有网络入侵检测、主机入侵检测，防火墙，病毒防护系统等。

事后处理是指系统遭到攻击之后能够进行安全恢复，能够对非法行为和误操作行为进行取证。事后的处理主要是定期进行系统备份，系统对所有的事件均进行记录（日志），并对日志进行分析审计，找出安全事件的原因。

2.2 安全管理体系的建设

据有关部门统计，在所有的计算机安全事件中，约有52%是人为因素造成的，25%由火灾、水灾等自然灾害引起，技术错误占10%，组织内部人员作案占10%，仅有3%左右是由外部不法人员的攻击造成。简单归类，属于管理方面的原因比重高达70%以上，这正应了人们常说的"三分技术，七分管理"的箴言。因此，解决网络与信息安全问题，不仅应从技术方面着手，更应加强网络信息安全的管理工作。

(1) 组织建设

应建立合适的网络安全管理组织，以保证在

组织内部开展和控制信息安全的实施。

安全组织管理体系由安全领导小组，安全专家小组，安全监察小组，安全管理人员，网络、系统、数据库管理人员，物理安全员组成。另外，信息安全不仅仅是上述组织的职责，每位员工在自己的日常工作中都有相应的保护信息安全的职责。

安全领导小组由公司管理层有关领导组成，以高层管理的身份，负责整个企业组织的网络安全的成功。

安全专家小组邀请国内相关领域的专家组成，其主要职责是对网络安全建设和管理提供咨询和帮助，并针对建设过程中遇到疑问或安全事件时提供参考意见。

安全监察小组由具有管理和运营经验的主管人员组成，其主要职责是对网络安全状况进行定期或不定期的监督检查。

安全管理人员指具体从事网络安全相关管理的人员，其主要职责是完成中国移动网络的安全体系建设，制定安全体系框架、安全技术规范和安全管理规章制度，对内部人员进行安全教育，并监督检查安全制度的执行。

网络、系统、数据库管理员负责具体的网络、系统和数据库的安全工作。

物理安全员负责物理安全的工作。

全体员工都有责任保护信息安全。

(2) 安全管理制度建设

面对网络信息系统安全的脆弱性，除在网络设计上增加安全服务功能，完善系统的安全保密措施外，还必须加强网络的安全管理制度。

制定安全管理制度，实施安全管理的原则为：

① 多人负责原则。每项与安全有关的活动都必须有两人或多人在场。这些人应是系统主管领导指派的，应忠诚可靠，能胜任此项工作。

② 任期有限原则。一般地讲，任何人最好不要长期担任与安全有关的职务。

③ 职责分离原则。除非系统主管领导批准，在信息处理系统工作的人员不要打听、了解或参与职责以外、与安全有关的任何事情。

(3) 安全管理的运作

网络安全运作管理是整个网络安全体系的驱动和执行环节。一个有效的网络安全组织会在网络安全策略的指导下，在网络安全技术的保障下，实施网络安全运作。

安全运作管理体系包括以下安全要素：

① 定期的安全风险评估。信息安全工作是一个持续的、长期的工作，需要定期进行安全风险评估，通过对安全管理策略、信息系统结构、网络、系统、数据库、业务应用等方面进行安全风险评估，确定所存在的安全隐患及安全事故对客户整体可能造成的损失程度和风险大小，了解在安全工作方面的缺陷，以及如何解决这些问题。

② 网络系统安全规划和项目的安全验收。为了将系统失效的风险降到最低，需要事先计划和准备以确保足够的容量和资源可用。应对未来容量需求做出预测，以降低系统超载的风险。同样，为了预先考虑和准备对于未来网络和信息安全问题导致系统遭到破坏，对于所有的网络系统都应当在该项目的开始阶段就引入信息安全方面的规划，在项目投入使用前进行安全验收。

③ 物理和环境安全。物理安全和环境安全是网络和系统安全的基础，有很多安全问题都可以简单地通过物理和环境的方法加以解决。

④ 数据备份。为了保持信息处理和通信服务的完整性和可用性，应建立常规程序以实施经过批准的备份策略，对数据作备份，演练备份资料的及时恢复，记录登录和登录失败事件，并在适当的情况下，监控设备环境。

⑤ 日志分析和安全审计。操作人员应该保留其行为日志。

⑥ 差错记录。对差错应该进行汇报并采取修正行动。应该记录用户所汇报的信息处理中或通信系统中的差错。

⑦ 意外和灾难恢复/入侵处理。通过对于意外、灾难和入侵的处理尽量减小安全事故和故障造成的损失，监督此类事件并吸取教训。影响安全的事故应该尽快通过适当的管理渠道报告。

⑧ 紧急响应体系。对安全事件的紧急响应的技术手段有日志分析、事件鉴别、灾难恢复、计算机犯罪取证、攻击者追踪等。紧急响应体系可以在最快的时间内对安全事件做出正确响应，保证业务连续性，也为事件追踪提供支持。

(4) 安全技术培训

安全技术培训是提高安全管理人员的安全技术水平，更好维护网管系统安全的一个重要方面。可以通过技术论坛、安全主题研讨会，定期进行安全技术培训和各安全厂商交流，接受安全服务等方式，把业务人员、安全管理员、以及安全主管领导的安全意识，安全技术水平提升到高的层次，更好的保证网络系统的安全、稳定的运行。

3 小结

电信行业的网络信息安全问题是一个长期存在的问题，它是包括管理和技术等多个层面的综合体。构架安全的信息系统时，应牢记如下指导思想："信息安全技术、信息安全产品是信息安全管理的基础，信息安全管理是信息安全的关键，人员管理是信息安全管理的核心，信息安全政策是进行信息安全管理的指导原则，信息安全管理体系是实现信息安全管理最为有效的手段。"同时任何网络安全和数据保护的防范措施都有一定的限度，一劳永逸的信息安全体系是不存在的。