首钢企业内部信息网络安全体系建设与发展

首钢自动化信息技术有限公司　郭雨春

企业内网安全建设的发展很不平衡，总体来看，存在以下薄弱环节：

(1) 人的观念问题有待提高，突出表现是没有把网络安全建设放到一个重要位置上来，主要表现为：

——从投资来看，网络安全的投入只占网络建设投资的很小一部分。

——先建网络，等出现问题时再考虑网络安全问题。

(2) 从被动防御转为主动防御，防患于未然的动作不明显，一般都是出了问题再解决，总是被动挨打，贼走关门。

(3) 网络安全问题越来越趋于商业化，这是一个值得认真关注的问题，许多病毒的始作俑者完全出于商业目的，其危害远远大于一般的恶作剧型。由此而引出的抵御、治理病毒的技术与成本也越来越大。

(4) 真出了大的网络安全问题怎么办？考虑不多。当然这也和网络应用范围、深度有关。

经过几年的努力，越来越多的企业进行信息化建设时，已经把网络安全做为重要内容来考虑。“设计时没有设计网络安全不准开工、没有安全建设的网络不准使用、出了网络安全问题查不清原因，不采取措施不准投入使用”的内网安全建设三不准原则越来越深入到企业的信息化建设中。

这些都说明，企业的信息化建设已经上升到了新的高度，并正在发挥越来越大的作用。首钢集团内部信息网络是一个构筑在以开放的网络协议和开放的系统平台为基础的网络系统。这种开放性给用户的使用带来了很多的便利，同时在内网安全问题上也带来了麻烦。

一、首钢内部网安全体系建设现状及存在问题

1. 网络系统的安全

(1) 划分安全的网络拓扑结构，利用网络层的访问控制技术实现对内部用户和外部用户的管理，隔离外部Web服务器群和内部服务器群，保证首钢内联网服务器的系统安全。

(2) 在Internett和首钢网络系统之间设立边界防火墙，外来用户只能访问倒非军事化区内特定服务器的特定服务，而不能进入内网。对于向外界提供信息发布的Web服务器，只开发HTTP协议，对于文件服务器只开放SMTP协议，对于FTP服务器，只开放FTP协议等。在网络系统内部设立内部应用服务器网络防火墙，利用防火墙对内部用户访问内部各应用系统进行控制，只开放用户必要的访问端口，对于来自内部的攻击可以有效地进行防范。

(3) 在计算中心设置入侵检测软件，监视对计算机中心服务器的访问请求，及时发现并阻断攻击企图。

(4) 在Internett和计算中心接口设置防毒网关，在网络入口处清除网络病毒的传播。

2. 使用系统的安全

(1) 确保公司在外地的分公司等机构通过Internet与内部网正常工作的安全。

(2) 确保公司外部计算中心与内部计算中心的数据安全交换。

(3) 确保防止数据泄密，主要指两方面：内部授权用户访问其授权范围之外的信息；内部用户对数据、信息的非法更改。

(4) 防止外部公众用户对数据、信息的非法访问，窃取内部数据信息。

(5) 确保数据的有效安全备份和非法窃取的数据不会被轻易解读。

(6) 安全系统的可监控性和易操作性。

3. 首钢内部网络防病毒体系结构

(1) 网络级防病毒。在网络环境下，防病毒必须层层设防，逐层

把关，堵住可能传播病毒的各种途径。另一方面，防范邮件病毒传播要加强对用户的安全教育，对于所有来源不明的邮件不要轻易打开，特别是其附带的邮件附件。

(2) 服务器防病毒。对重要的服务器，配置了服务器端防病毒软件。

(3) 主机及客户机防病毒。软盘和光盘是病毒传播的另一个主要途径，因此必须针对单机配置防病毒软件。针对病毒传播的各种途径配置防病毒软件，在内部网配置防病毒的管理中心。通过该管理中心对整个首钢内部网的防病毒系统进行统一的配置和管理，包括防护病毒软件包的自动分发和安装、病毒库的自动更新、病毒检测引擎的自动升级等。这些只需要管理员及时关注病毒的发展方向，及时下载最新的病毒库和病毒检测引擎，及时升级防护病毒管理中心的防病毒库，就可以把最新的防病毒库软件和病毒部署到整个内部网，及时查杀各种病毒。

(4) 应用层防病毒。应用层防病毒，是防病毒体系的重要环节，必须充分重视。由于应用系统的多样性和复杂样，不能以一种方式概括应用层的防病毒工作。除了必要的防护病毒软件之外，从人的素质抓起也是不可忽视的重要内容。单独依靠防病毒的想法是不切实际的，必须综合治理，配备相关的规章制度，严格实施，层层落实，才能达到目的。而且要使大家认识到，防病毒软件不是万能的，要改变认为安装了防病毒软件就可以万事大吉的错误认识，从根本上堵住病毒的传播途径。

4. 首钢内部网络目前存在的安全隐患

首钢企业内部网络系统是一个开放型的系统，与Internett连通后可能会受到外部的攻击。来自企业内部对网络的攻击也是不容忽视的。据统计，有97%的攻击是来自内部和内外勾结的攻击。权威数据表明，来自内部的攻击，其成功的可能性要远远大于来自 Internett 的攻击，其攻击的目标主要是获取企业的机密信息，如公司的发展规划、企业的人事、财务数据等，造成的损失要远远高于系统的破坏。外部攻击一般仅造成系统瘫痪，容易发现，不会造成数据的丢失，而内部攻击则经常是神不知鬼不觉，对数据的安全构成极大的威胁。

首钢应用系统也存在较大的安全风险，一些攻击者主要通过对应用服务器进行系统攻击，破坏操作系统或获取操作系统管理员的权限，再对应用系统进行攻击，以获取企业的重要数据。攻击者了解网络结构和系统应用模式，直接通过对应用模式的攻击，获取企业的机密信息，这些攻击包括：

(1) 非法用户获取应用系统的合法用户账号和口令，访问应用系统。

(2) 用户通过系统的合法账号，利用系统的BUG访问其授权范围以外的信息。

(3) 攻击者通过应用系统存在的后门和隐通道(如隐藏的超级用户账号、非公开的系统访问途径等)，从应用数据库或数据库服务器获取数据。

(4) 在数据传输过程中，通过窃听等方式获取数据包，通过分析、整合获取企业的机密信息。

这类攻击主要源于企业内部，包括通过授权使用应用系统的员工，开发、维护这些应用系统的员工、开发商等对系统进行攻击。

二、首钢内网安全的建设目标

针对目前存在的内网安全隐患，从2006年开始，首钢就开始了新一轮的内网安全建设，总的建设目标是六个字：关好门，管好人。从技术层面讲，是关好门；从管理制度层面讲，是管好人。

关好门就是在等级防护、积极防御与综合防范的安全策略下，以密码技术为核心，以安全管理为中心和密钥管理中心为支持构建的三重门：即应用环境安全、应用区域边界安全和网络通信安全。做到非法用户进不来，进来以后跑不掉。

管好人就是教育内部员工，遵守各项规章制度，并且有一套行之有效的管理办法。

整个内网安全的建设紧紧围绕“一个中心、两个平台”展开，即以集团信息中心为内网安全体系建设的中心，两个平台即是设备管理平台和风险管理平台。

——设备管理平台：通过有效的网管监控软件监控企业网路的各条链路状况、各个节点工作状况、各网络设备状态，对各项参数实施监控，提供各类故障实时报警，从网络通信链路方面保证应用的可用性、可靠性。

——风险管理平台：通过风险管理平台对全网的安全事件、安全策略、安全运维进行统一集中的监控、调度、预警和管理。

1. 首钢内网安全的下一步建设

安全系统建设的最终目的是保证核心业务应用系统的正常运行。因此，本安全设计方案是一个以应用层面安全、网络层面安全、安全管理与服务为核心的总体安全解决方案。统一应用安全平台是本安全方案应用层面安全的核心，它为核心业务系统的安全运行提供全面的应用安全服务，包括身份认证服务、安全访问控制、数据加密、解密服务、安全日志服务；网络层面的安全是在物理层、系统层和网络层保证安全的必要手段。

(1) 在网络层面我们将采用如下的安全策略：

——以防火墙为核心进行网络层面的安全部署。在核心数据区(内部服务器子网区)的前段部署高性能双层防火墙，严禁任何类型的业务用户不通

过防火墙直接访问到数据库，并配合负载均衡设备保障服务器子网的高可靠性。

——在重点网络接入区域或黑客入侵高发区域配合防火墙部署其它安全产品。在对外发布的服务器区如Web服务器，部署入侵监测器，增强对外服务器区的安全性。

——对首钢集团内网网络层的安全，采用先进的漏洞扫描和系统评估软件定期或不定期评估，根据评估报告采取相应的策略。

(2) 应用层面的安全策略。在应用层面我们将采用如下的安全策略：

——采用统一应用安全平台对所有应用系统进行统一的安全管理和防护。

——核心业务系统的安全软件开发中，侧重用户访问权限与日志审计的功能设计。

——针对不同类型的用户，采用不同的应用层面的安全策略。对远程用户的访问实施严格的身份认证审计、访问控制；对内部用户使用核心数据的全程进行数据加密和完整性检查；对核心数据如ERP系统的访问过程，进行详细的日志审计和数据加密等等。

2. 首钢内网安全管理与服务的安全策略

安全管理与服务将采用的重要安全策略如下：

——Internet访问控制管理：采用绿色通道产品和防火墙无缝连接，实现内部用户的访问控制。

——安全日志浏览审计管理：采用统一的日志管理平台对防火墙和安全日志统一管理。

——密码安全管理(从技术上考虑，可以设定用户的口令安全策略，可以分析用户的口令强度；从管理上考虑，建立口令使用的制度管理和奖罚机制)。

——成立安全工作小组，专门进行日常的安全设备管理和安全日志分析，经常性地使用各种攻击手段和方法检测网络设备的安全强度和用户口令的强度，根据分析结果采用不同的安全策略。这个安全工作小组，不是一个封闭的、可有可无的机构，而是一个开放的、具有实际意义的组织机构，这个小组在首钢集团的统一协调、领导下，吸收多家国内信息网络安全专业的单位与部门参加，为首钢内网安全运营、管理、培训提供服务，同时，为首钢内网安全管理制度的建立和执行，提供意见和建议以及必要的技术支持。

目前已经制定的制度有：

(1) 日常运维保障制度。建立完善的日常运维保障体系，从日常维护方面保证各项安全防护技术得以延续和发展。

(2) 安全管理保障制度。通过合理的人员组织结构的建设；各项安全规章制度、安全策略的制定；执行力度的监督管理等多项措施，从管理方面上保障安全防护顺利执行。

(3) 人员安全培训保障制度。通过定期的安全培训，从提高员工安全意识和保障安全防护水平的不断提高方面，进行内网安全培训教育，同时加强员工的安全技能培训。制度的落实，关键是人。员工的思想和行为都是在不断变化着的，“管好人”是整个内网安全建设中最难也是最关键的环节，再好的安全技术也要靠人来实现，而如果内部人员要想攻破它，也是比较容易实现的。结合企业信息化建设，我们已经摸索出一套在内网安全防护中，培训、管理人员方面行之有效的办法。

总之，要构筑一个企业的安全防护体系，必须从实体安全、防火墙、网络防病毒、入侵检测、核心防护、虚拟专用网、数据存储与备份以及灾难恢复、口令的安全性、系统的安全漏洞等方面建立起各级防护，构建一个完整的预防体系、完整的监视体系，并且要不断地改进、优化我们的安全防护体系。

三、首钢内网建设新思路

被动式的打补丁升级是我们一般采取的内网安全管理方式，从2006年开始，首钢内网安全建设以主动防御为目标，从建设可信网络开始，抓统一集中式管理，强化桌面设置管理，将首钢内网安全建设按照“国家信息安全保障体系”建设要求来进行，并超前一步来考虑内网安全问题，剑走偏锋，大胆实施内网安全建设的蓝海策略。其中一项重要的科研课题就是IPv6环境下的内网安全建设。

但是这一切都是在考虑如何布防、布控，而对于一旦出现的安全问题该怎么办？针对这一问题，我们未雨绸缪，从2007年开始，首钢将大规模开展首钢异地灾备工程建设，将首钢内网安全等级再提升一个数量级。

1. 建立首钢异地灾备系统

做好异地灾备系统的建设，首先要解决好本地的灾备问题。本地灾备系统一般采取系统定期检测与维护、双机热备、磁盘镜像、系统设备冗余以及定期进行人员培训及制度落实检查等手段。这样一来，会有不少灾难一般能够在系统发生故障后进行系统数据恢复，保证单位业务持续运行，不受到大的影响。与此同时，利用首钢本身的业务体系建设异地灾备系统，这套异地灾备系统我们称之为“小社会化异地灾备系统”，因为首钢集团本身就是一个很完整的体系，首钢总部与各个生产单位之间，各生产单位之间均可作为对方的异地灾备中心。这种方法不仅可行，其优势也十分显现：

——本系统内部的专业业务是相同的，沟通起来十分方便。

——有统一的指挥机构。

——这种你中有我，我中有你的灾备中心建设方式可以节省大量的维护费用与建设费用。如机房不用重复建设，不必增加大量维护人员等。

——灾备的测试和演练工作可以统一进行。

——制定统一的工作流程和管理建设，可以使日常灾备工作的出错率降到最低。

2. 端点安全防护体系的建设

在建设异地灾备系统的同时，企业内网端点安全防护建设正在抓紧进行。企业在进行网络安全建设进程中，一般采取的都是高筑墙方式，但是随着技术的进步以及信息化水平的不断提高，传统的网络边界变得日益模糊，同时企业业务的核心价值也不再是集中于核心服务器上，而是广泛分布在企业员工的电脑中，也就是网络的各个端点之中。这些端点可能会在任何时候、任何地点接入公司的网络，接触核心的业务信息，因此公司网络边界防护系统的构筑也变得愈发难以实现有效防护。

完整的安全端点控制系统应该能够对用户终端进行完备的安全状态评估，并对“危险”用户实行实时的隔离，该系统可以对用户终端的安全状态，即操作系统补丁，第三方软件版本、病毒库版本，是否感染病毒等反映终端防御能力的状态进行较为全面的评估，而不仅仅有防病毒等一两项功能；另外系统应该只允许符合企业安全标准的终端才能正常访问网络，如果不符合管理员设定的企业安全策略，只能被隔离或者访问病毒服务器补丁、补丁服务器等用于系统修复的网络资源，迫使“危险”终端用户及时升级自身的安全状态。在用户终端通过安全信息检查后，系统可能照用户角色权限规范用户的网络使用行为。当然，还有两个问题需要再明确一下。

(1) 端点安全防护的技术措施要根据企业的实际情况来制定宽与严的标准。

(2) 端点安全防护侧重的是边缘与端点，但这并不意味着就可以放松骨干和大型智能的网络设备的安全防护，二者不可偏废。这同样要根据企业的实际情况来决定。

什么是内网安全最佳解决方式？从厂商到用户都有不同的解释，但是从首钢内网安全建设的实践中我们悟出了一个道理，这就是：适用的、受本企业员工欢迎的内网安全解决方案就是最好的方案。CS

安全管理

1. 安全管理发展的驱动因素

作为IT治理的一部分，同时作为一种技术手段，安全管理其实很早就发展起来了。安全管理的发展是与企业IT信息化发展的程度息息相关的。试想，如果一个企业连IT网络基础设施都没有搭建起来，没有什么业务系统信息化，哪里有精力去考虑安全管理。经过多年的发展，国内的信息化基础设施都基本搭建完成。面对这些复杂的IT计算环境，管理尤其是安全管理，越来越成为制约企业信息化水平进一步提升的瓶颈。

除了前面提到的国内信息化飞速发展的内因，还有一个很重要的外因正在逐步显现，那就是法律法规和风险与内控管理。信息系统审计、内控与合规管理需求提升，直接刺激了安全管理系统的用户需求。近来，国资委、银监会、证监会、电信、移动、民航等等，纷纷发布了风险管理的相关法规和指引，都强调了IT信息系统安全管理的重要性，尤其提出了企业的一把手责任制。这种自上而下的压力迫使企业去搭建一套有效的安管平台。

基于上述内因和外因，以及其它相关因素，导致了目前安全管理市场不断升温。虽然目前国内市场尚未完全成熟，但是可以预见其强劲的发展潜力。

2. 安全管理技术发展的动态

安全管理，可以从IT治理的层面看，也可以从IT运行的层面看。在不同的层面，安全管理有着不同的内涵和外延。本文中的安全管理分析侧重于IT运行，并可作为落实IT安全治理的技术手段。针对目前的用户需求和市场，安全管理技术与产品有两条发展主线。

一条是以专一安全功能为主的安全管理产品。这类安管产品往往针对用户的某一类需求提供专业细致的解决方案。例如针对终端安全的内网管理系统，针对用户上网行为进行管理的网上行为审计系统，针对重要数据库操作控制的数据库审计系统等等。

另一条是面向IT计算环境的全面安全管理解决方案。这里，IT计算环境是指网络和安全基础设施、主机、服务器、支撑服务和应用中间件，以及业务运营系统在内的企业和组织所有IT设施的总和，它既有硬件，也有软件。计算环境还可以延