××研究院 ISMS 认证审核案例

推荐机构：中国信息安全认证中心

认证类型：信息安全管理体系

审核人员：路津（组长）

一、 审核背景

受审核方是××集团的研发大本营，是××技术体系的核心力量。××研究院注重人力资源建设、坚持技术创新和管理创新，并不断更新技术中心的软、硬件设备和信息化支持工具，具备了整套自主开发、独立研究创新和独立造型设计和CAE分析能力。为确保科研工作的顺利进行，和对自主研发成果的保护，2010年依据GB/T 22080-2008/ISO/IEC 27001:2005标准建立了信息安全管理体系。此次审核主要是信息安全体系的建立、实施，特别是信息安全控制措施的落实情况。

二、 审核过程及发现

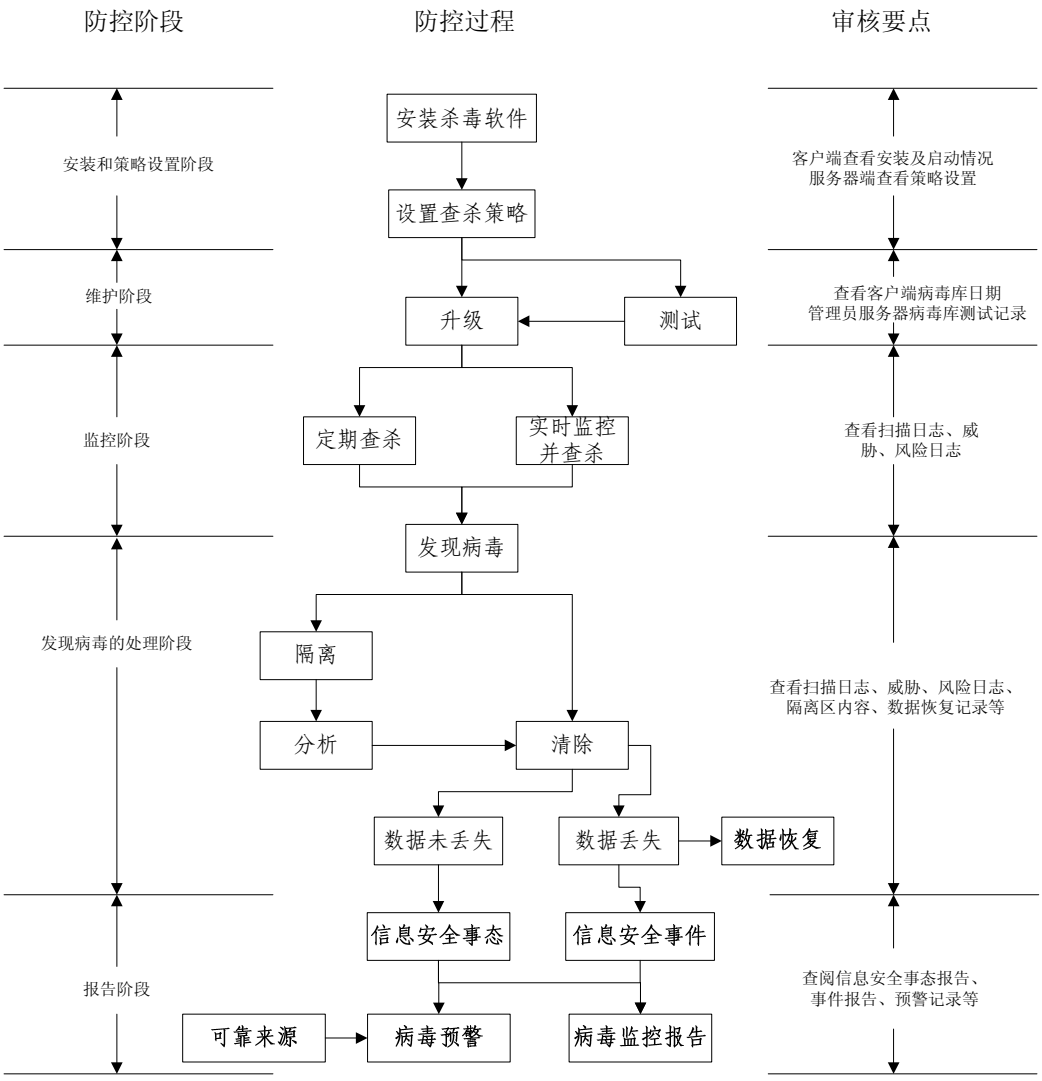
在审核研究院日常的安全管理的恶意代码的防控时发现存在漏洞和薄弱环节。

“恶意代码”是具有自我复制、自我传播能力，对计算机系统构成破坏的程序代码，大家称其为“病毒”，包括：传统病毒（引导区病毒、DOS 病毒等等）、木马程序、蠕虫、分布式拒绝服务攻击程序 DDoS、病毒产生器、垃圾邮件、恶作剧程序等，在网络中无处不在，无孔不入，是日常信息安全防范的最大的风险点。

在国标GB/T 22080-2008/ISO/IEC 27001:2005 A.10.4.1明确提出控制恶意代码 “应实施恶意代码的检测、预防和恢复的控制措施，以及适当的提高用户安全意识的规程” 的要求。

控制恶意代码除网络隔离、防火墙设置、限制移动介质使用、补丁升级策略外，在内网日常主要采用安装杀毒软件的方法来进行防控，其过程如下图：

恶意代码防控及审核要点流程图



中国信息安全认证中心　路津　2012.03.10

研究院依据标准制定了《防病毒管理程序》，并采用 XXX 杀毒软件对院内局域网内计算机防病毒进行统一管理。

但我们在审核时，发现：

1.研究院使用了大量的开发、设计工具，为保障其开发、设计过程，保护数据和成果，采用了内外网隔离技术。但为大家对外发送邮件和查阅资料的方便，在各部门设置了公用上网机（简称：公用机），公用机不在局域网管理之内，可随时上网，发送邮件、查阅网页、下载资料，但没有安装杀毒软件。

2.在查看病毒管理服务器 XXX 杀毒软件服务器端策略设置，“每天客户端进

行病毒库升级”，“每月一日 12:00 进行全盘查杀”，但对某开发部 IP 地址“***.***.***.199”的工作机的病毒库版本为 2011.4.25，查看病毒扫描日志时发现，已有 315 天未进行全盘查杀。

3．在某部门审核时发现，某工作人员工作机已感染病毒无法启动，正由防病毒管理人员对该机进行检查和病毒清除工作。询问工作人员日常是否关注防病毒软件的运行状况，并上报信息安全事态或事件，工作人员解释到：病毒防控是由服务器进行管控的，出问题找管理员，不需要自己处理，我们日常不关注，也不知道如何上报。

三、 审核沟通和分析

经与病毒服务器管理人员沟通了解到：

1. 研究院经综合考虑，统一采用XXX杀毒软件，在局域网内通过病毒检测服务器下发域策略到客户端进行统一的病毒防控的管理。
2. 由管理员负责对病毒库进行升级测试后，下发到客户端；
3. 日常有管理员查看服务器端病毒检测日志，每月发布病毒监控报告。
4. 而普通工作人员则认为病毒的检测由管理员统一管理，不需要个人去处理。于是出现了我们审核现场发现在恶意代码防护不同阶段出现的问题。

问题分析：

1、公用机未安装杀毒软件，四门大开，极易感染病毒，一旦染毒就会通过邮件、移动介质，传到局域网内，对工作造成困扰。公用机属于非生产环节，没有任何安全防范措施，反应出受审核方重视生产环节，轻视非生产环节的安全管理问题。

2、杀毒软件策略通过域控下发，应查看设备的通讯情况和其它域策略是否成功下发，排除人为因素；由于通信或其他技术导致的策略下发失败在实际工作也时有发生，除管理员加强用户核查外，使用者也应关注其病毒库升级的频次和定期查杀的启动情况，如有异常或长期未能及时升级病毒库情况，应及时与管理员联系，因为由于某些工作机由于工作需要

时常会使用移动介质进行信息的交换，如长期置之不理，极易感染病毒，对正常工作轻则造成困扰，重则造成数据丢失、损坏，甚至工作中断。这是杀毒软件域控策略下发时极易发生的问题。

3、使用者缺乏安全意识，日常不关注查毒软件的运行状况，特别是隔离区，隔离区会存放被病毒感染或疑似病毒的文件的副本，如不及时处理，也存在安全隐患，特别是反复出现的文件或病毒，更应关注，这反应问题的来源没有被查清并处理，需要分析原因彻底进行处置，管理员往往没有权限到使用者本机操作，需要使用者自己进行，对疑难情况可及时与管理员联系，由管理员协助。出现该现象亦应及时进行信息安全事态报告。

4、另外，使用者常常有一些错误的认识，只要安装的了杀毒软件能实时监控查杀，就不需要定期的全盘查杀。其实，杀毒软件是跟着病毒走的，先有病毒才会有病毒特征码，杀毒软件永远滞后于病毒，往往是中毒后才杀毒，所以定期的全盘扫描必不可少。另外，应建立消息预警机制，及时将可靠的病毒爆发信息进行公告，提醒使用者注意。

依据以上审核发现和问题分析，审核组开具了不符合项。

四、 改进及取得的成效

经以上分析，受审核组织领导对我们发现的问题欣然接受，并表示此次审核人员指出问题是工作中习以为常的，但却存在安全隐患的薄弱环节，一定认真整改。信息安全工作有木桶效应，哪块板短了，水就从哪漏掉了，因此应从细微之处着眼，未雨绸缪。现场审核后，受审核组织对提出的不符合项均进行原因分析并及时纠正，同时制定了纠正措施，举一反三，排查有同类问题一并整改，取得了良好的管理成效。

改进过程：

首先：对公用机安装XXX杀毒软件，并进行全盘扫描；对于未在域控策略之下工作机，已经重装系统，经测试可连接上XXX杀毒软件的控制中心，能够接受域控策略，并能按期启动全盘查杀；同时，举一反三要求各部门核查工作机中XXX杀毒软件，是否均在域控策略之下，并定期进行全盘查杀，对于未能进行的电脑

核查原因并重新恢复。

问题纠正后，又完善了《防病毒管理程序》，补充了病毒处理方式、病毒预警和报告机制等内容，同时对全体人员进行了培训，要求使用人员日常做好备份工作，并关注病毒库的升级、查杀及日志记录情况，同时普及了信息安全事态和信息安全事件的报告机制。

取得的成效：

提高了人员的安全意识，改变了一些工作人员认为只要安装杀毒软件就一劳永逸和病毒查杀由服务器统一管控就是一切事项均有管理员一人负责的错误认识，杀毒软件不仅要安装，更要及时升级；病毒查杀软件的运行和良好的处理，也不仅需要管理员认真负责，更需要每一位使用者日常的关注和维护，才能起到对恶意代码的有效防控作用。

另外，大多受审核方都非常关注生产环节的信息安全管理，而对于非生产环节的信息系统的管理则相对薄弱，如此次受审核方的公用机，就属非生产环节（研发、设计系统），在实际工作中非生产环节计算机往往会保存生产环节直接相关的信息如网络拓扑图、日常工作分析报表等，如被不良企图人得到并利用，会对生产环节的安全形成无法预计的安全隐患，因此管理层不仅要关注生产环节的信息安全，也要对非生产环节的安全进行严格的管理。

五、 总结

过去企业内部，信息系统只是设计、开发的工具，对存储的设计数据、图纸的保护，不引人关注，随着各种开发、设计、测试、及办公系统的应用，业务的连续性，数据的安全性，企业的运营、各种技术和商业信息的保护迫在眉睫。企业领导审时度势、未雨绸缪，建立并有效地实施了信息安全管理体系，在付出一定管理成本的同时取得了可喜的社会效益：

1、 首先，为日常产品开发、设计等正常工作秩序提供了一套系统、有效的保障机制；

2、 其次，开发、设计、测试数据统一管理，减少了技术人员流动给企业技术研发带来的冲击；

使企业的各种专利技术得到有效的保护，不丢失、不被窃取、不被盗用，增强了企业在市场上的公平竞争实力，提高了企业的社会效益。