方案基本内容:收集硬件信息及设备使用情况,对内存、CPU、硬盘等硬件属性信息变化进行监视、报警

1. 了解:什么是安全审计
2. 目的(好处):为什么做内网安全审计

   企业重要的文件资料、专利设计等防窃取、防篡改、防病毒等。
3. 内网安全审计的范围
   a. 终端审计
   b. 邮件审计
   c. 数据库审计

   三大类:数据库操作的行为、办公OA操作的行为和系统网络维护的操作行为。
4. 需求分析:根据不同需求制定方案
   (面向业务的信息安全审计——银行、保险、证券、移动等)
5. 审计过程:个人调查、漏洞扫描、操作系统和安全设备的检查、网络分析、检查事件日志中的过往数据。

   证据——分析——报告

局域网安全审计方案

1. 目标

企业内部网络一般都是涉密网络,要求保证涉密信息的绝对安全,一方面通过制定严格的制度加以防备,而更可靠的手段还必须依靠技能防备。涉及国家秘密、单位秘密的计算机系统安全防备的最佳手段就是采用“物理隔离”,即将单位内部网络与外部网络、互联网实现物理上的隔离。

物理隔离可以防止来自外部的网络攻击，但对来自企业内网的网络安全威胁。仍然需要采取必须的安全防备要领和安全审计系统软件。

内网安全审计是一种基于信息流的数据采集、分析、识别和资源的审计方式，通过实时审计网络数据流，根据用户设定的安全控制策略，对受控对象的活动进行审计，对内网重要数据和资源的全局控制、把握和调度能力。

安全审计的目的就是保证企业信息安全，风险管理和调整兼容性方面达到完美的境地，安全审计可以反映企业在技术、实际操作、雇员或是其它关键安全领域的一些缺陷，安全审计在帮助企业更加经济有效地保护企业软硬件安全方面有很大的作用，还有助于企业更好地发挥安全技术和设备在实际应用中的表现。

一、网络安全现状

随着网络规模的不断扩充，企业内网中部署了越来越多的网络设备、服务器、主机、数据库和应用系统等，在为自身业务提供高效的网络运营平台同时，日趋复杂的ＩＴ业务系统与不同背景业务用户的行为也给网络带来了潜在的威胁。

国外的一项安全调查显示，超过85%的网络安全威胁来自于内部，其危害程度更是远远
超过黑客攻击及病毒造成的损失，而这些威胁绝大部分是内部各种非法和违规的操作行为所造成的。内网应用中对各种资源(主机、数据库、服务器等)的滥用、误用、恶用行为，正在日益损害业务的正常运营。为了有效降低来自内部的安全威胁，内网需要构建操作行为合规性审计体系，以达到对操作风险有效控制的目的。

二、内网安全审计需求分析

最初，部署审计系统与产品的目的在于提供安全事件的事后取证机制，定位安全事件的责任人。这种功能单一的审计体系基本上能够满足普通的应用场合，但对于像金融、证券、运营商、大型企业等核心业务实时依赖于各种信息系统的用户而言，就作用不大。因为各种信息系统或数据系统中的违规操作行为，如果不能被及时发现与控制，就可能为企业和国家带来巨大的资产与名誉损失，甚至需要承担法律上的责任。这就对审计系统提出了实时监控的要求，而不仅满足在安全事故发生以后，对于违规操作行为责任人的查找和取证。未雨绸缪、防患于未然远比简单的亡羊补牢重要。

另外，从用户的安全审计需求趋势来看，内网合规性审计正越来越受到用户的重视与认可。合规性审计不仅意味着要符合相关的行业安全条款与标准(如金融行业的《巴塞尔新资本协定》、银监会颁发的《国有商业银行公司治理及相关监管指引》、在美国上市须遵循的《萨班斯法案》等等)，还要能够灵活适应内网安全现状与业务信息系统特点。同时，内网安全审计必须与安全策略的制订与落实紧密结合在一起才有意义，简言之，安全审计要能够针对内网中的访问与操作行为制定相应的行为策略与约束条件，关注重要的内网操作行为风险。

1.2 安全审计范围

内网安全审计:

1.拨号审计

2.文件操作审计

3.系统日志审计

4.进程审计

5.打印审计

6.主机IP/盘符审计

7.邮件审计

8.主机IP地址审计监控

9.数据库审计监控

10.数据库远程操作审计

11.数据库远程管理审计

主机审计

主机审计子系统设计的主要功能有:

(1)系统信息综合审计功能

对系统的配置信息和运行情况进行审计,包括主机机器名、网络配置、用户登录、进程情况、CPU和内存使用情况、硬盘容量等。

(2)网络连接审计与保护功能

网络功能审计包括:对主机网络实时信息的审计、设置网络规则和查询网络日志信息的功能。记录和审计主机的网络连接情况,审计主机开启的服务,制定网络连接规则,允许或禁止指定的网络连接,对数据包内容进行过滤,非法的连接产生报警事件。能够有效的发现网络内部新接入的访问数据的计算机,并发出报警。

(3)拨号审计功能

□□

对Modem进行审计,任何方式的拨号都将禁止,可以设定规则在特定时间内让特定的号码允许拨出。同时,记录任何允许和禁止的拨号事件。

(4)文件操作审计

能够有效监控终端计算机共享文件目录的访问情况,可记录到源ip、用户、执行的操作等最基本的层次。在驱动级对客户端的文件读、写、删除、移动、拷贝等操

作进行审计，比如能够对用户访问doc、txt等各种格式文件的操作进行记录或报警。

(5)系统日志审计

□□

系统日志审计包括:系统日志、安全日志、应用程序写入的系统日志、其他服务(如DNS Server)日志等，同时对系统日志进行查询和管理。

(6)进程审计

□□

设置进程为合法或非法后，提供非法进程实时报警和报警信息查询功能。对系统进程进行实时审计，当出现没有被网络管理人员定义为合法的进程启动时，系统会产生进程报警信息。

(7)打印审计

□□

对各主机的打印操作进行审计，包括打印机名称、打印机位置、打印对象、打印份数及打印用户和打印时间等;同时还可以对打印进行控制，允许或禁止打印。

(8)主机IP/盘符审计

对被审计主机的 IP

地址修改进行记录和禁止。同时可以查询指定时间段内被审计主机 的IP

地址修改信息。

□□

并且可以控制和管理光驱、软驱及USB接口使用;对于违规事件，系统会产生报警信息。

(9)邮件审计

□□

对各主机基于pop3协议的邮件收发进行审计，用于实时监控和事后查询邮件操作。可审计内容包括邮件日期、收发者及主题等。

(10) 对文件操作监测的控制功能

严格控制文件的操作，保证不同级别的人员和部门拥有不同的权限，包括复制、保存、另存为等。措施如下：

a.防止文件拷贝(只有受权者才可以拷贝);

b.控制“保存”和“另存为”操作(只有受权者才可以保存)，并且防止屏幕拷贝;

c.设置文件的利用有效时间

d.重要电子文档在限定用户阅读范围基础上，附加指定在哪些机器上允许阅读(根据机器名、某段IP地址、MAC地址的一个或多个组合)

(11) 对于外部设备监测的控制功能

对于部门内部的计算机，根据不同的需求，阻断对外的接口。

网络审计

网络审计子系统的主要功能如下：

(1)网络入侵检测功能

对从网络中抓取到的包进行协议分析，与相应的入侵检测规则库进行模式匹配，从而发现有入侵特征的数据包;同时记忆基于连接的网络数据包前后状态，从中分析入侵的可能或企图。发现入侵或可疑企图即产生入侵事件。

(2)协议审计功能

此功能对应用协议的操作和内容进行进一步的分析，对有特殊内容或某些违规的操作产生报警事件。管理员可以定义违反规则的内容策略，在匹配到相应内容后记录并产生报警事件通知管理员。

（3）流量统计功能

对抓取的数据包根据某一类（如IP地址、MAC地址、URL等）进行归类统计，可以得到各种流量统计表或统计图。可以对某些地址的流量速度进行限制，超过规定值时即产生报警事件。

(4)对加密数据进行审计

克服数据包类型的差别和加密和复杂程序，可以截获并控制过滤数据包的流量内容。

（5）MAC地址绑定功能

制定IP地址与MAC地址的对应关系，如果抓取到的数据包与此对应关系不符，则产生报警事件。

数据库审计

数据库审计系统采用网络传感器组件，对特定的连接数据包（数据库远程连接）进行分析，从数据库访问操作入手，对抓到的数据包进行语法分析，从而审计对数据库中的哪些数据进行操作，可以对特定的数据操作制定规则，产生报警事件。

由于数据库系统的种类比较多，所以数据库审计从网络方面入手，监控数据库的操作。可以审计所有的远程数据库操作，通过旁路技术实现审计。

数据库审计子系统的网络审计功能通过对数据包中数据操作语法的分析，可以知道对数据库中的某个表、某个字段进行了什么操作，并可对违规的操作产生报警事件。

(1)数据库远程操作审计

通过对数据包中数据操作语法的分析，可以知道对数据库中的某个表、某个字段进行了什么操作，并可对违规的操作产生报警事件。

(2)数据库远程管理审计

对数据库系统本身所产生的日志文件进行审计，达到远程管理数据库的目的。

//**********

终端审计的真正目的在于通过终端一些异常行为进行分析，及时发现内网安全管理的脆弱点，并对一些恶意行为进行取证和警示，保证内网安全渐趋完善。因此，如何加强对主机的安全监控和管理，成为了企业内网安全建设的关键之一。

内部资产统计：自动登记受控终端的硬件配置（包括CPU、内存、硬盘、显示卡、网卡等）当受控终端的硬件发生变动时能自动发出告警信息。

系统配置信息统计：记录受控终端操作系统配置的用户、工作组、逻辑驱动器发生变化报警。

其它信息功能统计

·自动登记客户端补丁安装情况，已安装补丁和未安装补丁列表显示；

·对受控终端的系统服务、应用程序的安装与卸载情况及进程进行审计，自动记录其操作行为的变更；

·通过安全管理核心平台可以随时查看受控终端的系统日志，包括应用程序事件、安全性事件和系统事件；

·对网络访问进行审计，记录用户对规则指定网址进行的访问操作；

·对打印机使用情况进行审计；

·对受控终端的软盘、U盘等移动存储设备的使用情况进行审计；

·对拨号访问情况进行审计；

·对受控终端的共享文件夹设置进行审计，包括共享、会话和打开文件的信息；

·查看受控终端的TCP/UDP连接端口，及时掌握受控终端的网络连接情况。

**********//

2. 依据

ISO-7498-2(信息安全技术框架)

ISO/IEC15408(通用评估标准)

ISO/IEC10181-7:1996(信息技术—开放系统互连——开放系统的安全框架)

ISO/IEC 10164-8:1993(信息技术——开放系统互连——系统管理)

国标GB/T 17143.8

国际上对强审计非常重视，在ISO-7498-2(信息安全技术框架)和ISO/IEC15408(通用评估标准)中，已将审计作为一类重要的信息安全机制或功能，可见，国际上非常重视信息安全的审计。同时在ISO/IEC 10181-7:1996(信息技术—开放系统互连——开放系统的安全框架)中已经规定了安全审计和告警的框架;在ISO/IEC 10164-8:1993(信息技术——开放系统互连——系统管理)第8部分，也说明了审计系统应有的功能，这个标准1997年已经变成了国标GB/T 17143.8。