从证券业安全大检查的一点经验谈起思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/629/2021_2022__E4_BB_8E_E8_AF_81_E5_88_B8_E4_c101_629010.htm 今年以来，我国股市接连受到重挫，造成了部分股民的不满，同时也出现了针对证券公司进行网络攻击的恶性事件。因此，证监会组织了对全国证券业的安全大检查。笔者因为工作原因，参与并负责了几个大型证券公司的安全检查。检查的从体情况来看，有喜有忧。喜的是证券业前几年行情不好，一直没有资金进行充分的IT基础建设，造成IT建设欠债太多，但最近两年已经迎头赶上，并且证券业创新产品层出不穷。忧的是这两年券商的IT部门一直被赶着做事情，又造成对信息安全问题重视不够，出现了很多新的风险，尤其在当前股市震荡的情况下，威胁越来越大。它山之石可以攻玉，对于各个行业的安全管理员来说，保障信息安全是一个任重而道远的工作。本文基于在证券业安全问题上的一些经验和思考，希望也能够给其他行业的安全管理员提供帮助。 整个安全大检查从几个方面进行了审查，包括网站安全、物理安全、网络安全、系统安全和管理安全。 一、网站安全 证监会组织了人手对所有券商的网站进行了渗透测试（模拟黑客攻击的方法对网站攻击，但不做破坏性举动），虽然最后证监会没有公布网站渗透测试的结果，但就笔者负责的4个券商安全检查来看，全部都被攻陷，被攻陷的方法全都是sql注入，并且还发现了源代码泄露、跨站漏洞等问题。所幸的是，经过检查，没有发现这几个网站被人入侵过或者有什么远程后门。总的来看，大家对安全补丁、系统自身的加固都很重视，没发现什么明显

疏忽，但是在WEB的安全编程上还做得远远不够。究其原因，由于券商自身不具备网站开发能力，网站开发都是外包来做，而外包公司在程序的代码审核上做的远远不够，代码中可能的漏洞有溢出漏洞、跨站脚本漏洞、SQL注入漏洞等，还有一些因为程序设计不周到而导致的信息泄露问题也应该得到重视，这些漏洞本身可能没什么大的威胁，但非常有助于攻击者利用其他漏洞进行攻击。当前总体的网络安全状态是基于操作系统本身漏洞的入侵已经没有大的增加，而由于应用系统的复杂性和特异性，基于应用的入侵已大幅度增加，所以在这方面还有许多需要加强的工作。 从证券业的网站安全来看，入侵甚至在C盘根目录上写入文件，都不是什么难事。笔者在其他一些行业的评估中，也发现同样问题的存在，并且今年的安全形势报告中也提到，仅在5月份，全国就有12万网站受到sql注入式的攻击。因此可见，面对新型的攻击手段，安全部门响应速度迟缓。网站是一个企业的门面，如果网站被篡改，带来的负面影响会很大，加强网站的安全防护，应是当务之急。 二、物理安全 物理安全作为信息安全的基础，在整个信息安全体系建设中扮演着非常重要的作用，而物理安全的好坏直接影响到网络安全、系统安全和安全管理等等层面。对于券商来说，机房是生产的核心工具，这几年来，管理层对此也不断提出要求，目前看来，硬件环境已经比较可靠，空调、湿度控制、防火、区域标识等相对完善，但与之相对应的软件环境却不甚乐观。比如普遍存在的：2.1 环境 机房进出控制等级没有严格执行，流于形式；门禁系统虽有，但时常进出没有随手关门；进出人员所做重大操作没有记录；第三方人员进入机房没有明显的可视标识，

不能立即识别出无人护送的访问者和未佩戴可视标识的人。 2.2 设备 网络设备、主机设备没有有效的标记措施，对资产的界定不清晰；重要的主机设备没有防盗报警措施；由于券商在不断地上新项目，经常需要调整网络，网线和电缆的普遍走线比较乱，很多网线、电缆都没有可识别的记号。 2.3 介质 对移动存储设备没有实行有效管理，各服务器的USB口都是开放状态。 没有对移动存储设备上的敏感数据彻底删除或安全重写。 这些问题在很多公司机房都普遍存在，甚至比证券业要差很多。安全不仅仅是网络安全，更是一个整体的木桶，任何的短板都会导致前功尽弃，加强对物理环境的管控应是踏踏实实要做好的事情，这种管控也不仅仅是在硬环境上，更重要的还在软环境上。 三、网络安全 近年来证券整体行业效益不错，因此在网络上投入很大，起点较高，并且由于券商大多数都是跨地域的，整个IP地址的规划也都比较合理，具有连续性，能够与网络拓扑层次结构相适应，便于进行管理。作为网络建设重要规范性之一的可靠性建设也受到很大重视，针对故障恢复、承载能力以及安全配置均充分考虑了关键网络设备和重要链路的可靠性建设：通过交换机之间Trunk互联和专用负载均衡设备，实现动态的冗余热备和流量分担，有效提高了网络的可靠性和可用性。对于重要的主机设备同样部署了完善的链路和设备双备份，通过双归属方式的互联和采用主备设备的方式，可确保一旦出现问题可以实现快速的切换，把对业务的不利影响降低。同时在交换机上根据业务的需要划分了相应的VLAN，通过二层隔离有效杜绝了蠕虫病毒的扩散和广播、组播数据流的防洪，提高了网络的安全和承载效率，确保网络系统具有了良好的扩展性

和健壮性。 但是安全问题也总是伴随着网络建设而来，创新业务不断出现也要求对外的接口越来越多，例如对各个银行、上交所、深交所的接口。在出口很多的问题下需要认真对待各出口的分界线控制，这方面，已经有很多机构提出了安全域架构的方法，在实践中也取得了认可。 再有就是对网络保密的情况考虑不足，在这方面银行走在了前面，对链路都是由加密机来加密。券商对此尚没有顾及，关键的业务数据在传输时zheng没有加密手段，可能被监听泄露。据笔者和各信息部门老总交流的情况看，也并不是没有考虑，他们担心加密以后对网络的实时性造成影响，而且券商内跑的应用很多，业务系统与加密机的配合会不会出问题，再者，券商的网络多是专线连接，被窃听的可能并不很大。我承认，老总们的担忧很有道理，在现有技术情况下，如何进行无障碍的链路加密？这也是咱们国内的安全厂家应该去深入研究的课题。 还有一方面就是对网络的管理：目前的网络设备基本都具备日志功能，但是由于人手不足，业务繁忙，管理粗放都很多原因，并没有人去定期核查这些日志信息，也没有专用终端记录处理日志，这会造成即使已经被攻击了，管理人员仍然不知道。并且在网络管理上没有指定专用终端操作，为了方便很多机器都可以连上去更改配置。 四、系统安全 券商核心业务系统多是LINUX、HP-UX等，这些系统流行面较窄，精通该类系统的人不多，且由于系统的不兼容性使得受攻击的可能性大大降低。但同时，也由于大家都不精通，系统上发现的一些已知的安全补丁都没打，不是不知道安全漏洞，而是因为不敢做，做了以后会对应用产生什么样的影响大家都不知道。这种情况在很多行业都存在，比如近期我接触

过的一个煤矿有个瓦斯监控系统，1分钟都不能停。这种形势下，就要求对核心生产设备做足够的外围安全防护。 还有一个老生常谈的话题就是口令安全，网络设备口令、操作系统口令、应用系统口令、数据库口令等等，实际对口令的管理和要求始终会有差别。在调研中，我们也和老总们谈过，大家都说：我们都知道口令的管理，也知道怎么加强，但在实际中要考虑证券公司的特殊性，例如报盘系统登陆易所，20多个席位要登录，有一次系统意外重启，我们每个席位口令都很长，够复杂，结果手忙脚乱地往里面登录，一边看一边敲，敲错了还要重来，最后都搞好，半个小时过去了，所以这种安全手段在证券公司没法考虑的。 非核心业务的其他终端设备受系统升级和疏于管理等问题，普遍存在着非常多的高风险漏洞，甚至包括操作系统级的弱口令。不过目前对证券业来说，基本都做到了业务的主辅分离，所以威胁有，但不是很大。既便如此，非核心系统也应给以更多的关注。