网络安全管理层面安全管控措施

赵建刚

广发银行石家庄分行，中国·河北　石家庄　050000

【摘　要】随着经济的飞速发展，金融业已经逐渐占据我国主体经济地位，金融业的管理逐渐网络化、数字化、智能化，这种发展成为了新一轮的科技革命，信息化、网络化已成为现代金融的重要发展方向。相对应金融网络安全风险也在不断涌现，对金融业网络管理方面造成严重的威胁，对其安全管控已经刻不容缓。

【关键词】金融业；网络管理层面；管控措施

Network Security Management Layer Security Control Measures

Zhao Jiangang

Shijiazhuang Branch of Guangfa Bank, Shijiazhuang, Hebei

[Abstract]With the rapid development of economy, the financial industry has gradually occupied the main economic status. The management of the financial industry has gradually been networked, digitized, intelligent. This development has become a new round of scientific and technological revolution, information, network has become the important development direction of modern finance. Corresponding to the financial network security risks are also emerging, causing a serious threat to the financial network management, its security control has become urgent.

[Keywords]Financial industry; Network management layer; controls

金融业是我国重要经济体，对于公众的生活有着巨大的益处，承担着多方面的责任。比如存取款、征信查询、资金结算等。金融业的发展情况和安全情况在一定程度上会直接影响到公众的生活，一旦出现安全问题，所造成的损失是巨大的，轻则损失公众财产，重则会影响社会资金流动，耽误发展进程。所以，对金融业网络管理层面的安全管理重要性不言而喻，本文围绕金融业网络管理层面，对其的隐患和安全管理措施进行探讨[1]。

1　金融网络安全现状

1.1 国家安全战略要求提升

随着信息技术的发展，金融业网络管理方式已经成为主流，对于其安全情况，关系到国家和人们的利益。特别是随着《网络安全法》的颁布，国家对金融安全方面十分关注，对主管责任、安全建设、数据保护方面都制定了明确的标准，提出了明确的要求。要求能在新时代社会发展下做好对金融业网络安全的保障工作。对于金融业网络安全的管理方面而言，企业本身一定要清晰认识到自己的责任，建设出完善安全的管理体系，在风险的角度去看待网络安全管理，避免安全隐患的出现，使得金融业可以进行持续性发展，为人们的经济安全作出保障。

1.2 网络威胁日渐严重

近些年来，随着科技手段的发展，网络上出现了大批新型网络威胁，并且这种方式通过互联网进行金融犯罪，个别网络罪犯还隐藏了IP地址，使得无法进行抓捕。而金融组织机构成为了网络罪犯的首要针对目标。同时，网络威胁的形式非常严重，通过各种各样的互联网攻击技术对金融业管理系统进行打击，因此而发生的金融案件不在少数。围绕着互联网的一些黑灰色产业正在以极快的速度在各公司之间进行渗透，甚至涉及到了国家方面。随着网络罪犯的增长，所受到的经济损失也越来越多，对于公众的经济都产生了威胁。每年发生的网络攻击事件都在不断增长，经济损失已达到千亿级别[2]。

1.3 金融科技发展带来阻碍

金融科技正在从后台向业务方向发展，随着技术与业务的融合，的确创新了金融业的部分方面，给金融业的服务和产品方面进行了一定的推动，但是随着利益而来的还有金融网络安全方面的诸多问题。在网络发展的背景下，金融业的业务系统也随之发生改变，系统的开发架构正在转变，对产品的上线和灵活性有更高要求，但是也会导致风险增加。对于网络的使用要考虑到除却传统安全系统外的私有保证系统。如何有效的防护和处理都是需要解决的问题。大数据成为金融核心的同时，也要有效治理数据泄露等方面的问题，但因为新兴技术的出现导致发展形式越来越严峻。

1.4 传统网络安全威胁仍旧存在

传统网络威胁仍旧错在，以分布式拒绝服务为例子，根据研究调查，发现金融行业内有三分之一以上的机构收到过此类网络攻击，并且这种占比还在持续增加。同时因为网络发展的普及，各种分析、扫描、破解方面的网络工具可以随意下载，就导致越来越多的黑客涌现出来。金融机构每天都会受到大量的侵扰，一旦出现安全隐患，就会被各种不同类型的恶意分子进行攻击，如果未能有效治理，就会造成破坏性的影响。

2　金融网络管理安全威胁分析

金融业网络管理层面遇到的威胁多种多样，可以通过多种方式多种渠道对金融业的发展造成影响，造成经济损失，大体分为以下三个方面：

2.1系统不完善

关于金融系统的安全开发一直都存在着一些问题，下面进行两个方面的讲述：

一就是系统开发安全生命周期管理。金融安全系统的开发存在着许多问题，很多机构对软件的开发不重视，缺少完善的安全管理体系，没有办法有效控制风险，导致出现安全漏洞，不但会影响金融网络系统的运行，也无法保证安全管理。此外，金融机构缺少高效安全系统开发途径。不能保证及时对安全系统进行改善。二是各类系统存在漏洞，因为金融系统资产繁杂，所以除去相关系统，也会借助其他系统进行整理，造成资产识别和管理困难，需要升级时，无法进行选择[3]。

2.2外界因素

外界因素威胁大体分为四个方面。第一方面就是持续性攻击，这种攻击的组织性和目的性都很强，有着强有力的后台支撑，甚至是国家在幕后推动。这种威胁的隐蔽性极强，潜伏时间长，无法及时发现。这种威胁通常针对核心系统中的数据资产，一旦金融网络安全系统被攻克，后果不堪设想。第二方面就是恶意代码，这种威胁的形式十分多变，包括病毒、木马等多种方式进行攻击，这种最常见的攻击手段却最容易让人大意。第三方面就是DDoS攻击，这种攻击很传统，但是攻击频率十分高，模式多样，不易防御。针对中小型金融机构进行影响，对其的持续攻击性极强。第四方面就是软件供应链攻击，是指在下载合法软件时，利用软件供应商的漏洞进行篡改，借用安全软件躲避检查，这种方式在网络上十分常见，大到金融产业，小到家庭使用。

2.3内部原因

金融网络管理出现问题的内部原因主要分为有三个：

一是操作失误。内部人员没有按照流程进行使用导致系统瘫痪，会无法对外进行服务，甚至是重要数据损坏，发生这种情况的主要原因就是内部人员的操作技术不达标，缺乏安全意识，无法胜任任务，对工作内容不负责。

二是内部恶意人员。有些内部人员可能收取他人的利益或者就是被指派的卧底，通过盗窃数据或者篡改数据的方式来取得利益，根据统计，数据泄露是大多金融机构最常见也是最严重的问题，一旦发生，不止损失数据，对其声誉形象都会产生影响。

三是软硬件故障。受到物理环境的影响，导致无法正常运行安全系统，许多原因都会导致软硬件，例如潮湿、断电、灰尘等。

3 金融业网络管理层面安全管控建议

3.1提升安全意识

为满足网络安全要求，需加强网络安全意识教育工作，保证全员安全意识到位。并利用好保护测评、风险评估、测试审计等手段，对自身进行分析，保证每个资源在遇到危险时能够做出及时的调整，构建安全机构风险管理体系。

3.2转变思维，建设安全管理体系

威胁不是稳定的，会不断进行变化，因为应当未雨绸缪，将安全理念贯彻到整个安全系统。特别是针对开发者方面，要保证对每项数据都严格掌控；其次，要有被攻击的觉悟，随时做好防御准备；最后，要主动养成防御思维，被动的防火墙无法应对多样的网络安全威胁，因此要弹性面对威胁，构建安全体系，来应对各种威胁。

3.3合作进取

在互联网的飞速发展下啊，国家和行业中出现了一批专控队伍和安全厂商，他们能够有效的防止金融安全问题的出现，彼此之间可以构成一张安全网，对网络安全产业进行分工处理。这批网络精英借助技术优势没探索国内外安全技术，并加以学习应用，与金融产业开展合作，形成安全网络链，有效保证金融业发展。针对各种外部攻击和威胁，共同建立网络安全机制，构建一体化的技术体系，为国家金融产业的网络安全工作进行推动[4]。

4 金融业网络管理层面安全管控的具体措施

4.1 部署防火墙。

防火墙是预防威胁攻击的有效手段。一般部署在核心路由器和交换机之间，通过路由模式或者透明模式进行地址转换，通过企业中心连接内部数据，保证数据访问的安全性。

对外部边界部署区域提供防火墙。防火墙的工作模式应当设置为路由模式，保证防火墙的数据能够安全有效的进行地址转换，对国际用户、外机构访问企业内部服务、资源进行有效控制。

对内部部署专网防火墙。全部都配备双机热备并按照端口级的最小限制进行授权，再对访问控制安全策略进行配置。

4.2区域防护

对于整个金融产业的划分可以分为不同区域，面对不同区域实行不同类型的物理隔离：在核心区域放置核心网络设备，例如核心路由器和核心交换机；在员工工作区放置个人办公需要的电子设备；在生产区放置一些内页内部所需要的应用设备；安全区内设置安全设备，例如预防警示、受攻击警示等等，保证及时有效发现问题；管理区域布放一些网管或类似的管理应用。这些区域需要有明确的区分，多数工作内容不一样的就进行物理分区，出现个别特殊区域可以不进行物理分区，例如功能重叠的可以进行逻辑分区。各区域之间要分开运行，保证责任落实到每一个部门，每一个人的身上。但是又要保证在区域之间要有一定联系，保证能够通过安全控制策略对传输服务的管理[5]。

4.3网络设备安全

4.3.1防地址欺诈

在路由器上设立一定的ACL访问控制，并结合一定的筛选，运用到目标端口。在交换机上，实现IP地址绑定。绑定以后，黑客就无法利用模仿IP来逃避检查，进行盗取或损害金融数据的行为，这种技术的使用很大程度上防止了访问系统被攻克出现的问题出现。

4.3.2过滤攻击端口

常见的攻击包括蠕虫、震荡波等，可以利用ACL对UDP及TCP端口进行抓取，然后在设置关键字，通过匹配关键字，应用到设备上联端口。这种方式类似于密码设定，属于基础过滤方法。

4.3.3日志记录

配置日志服务器，在通过一定的设置，通向该服务区。金融业的日志比较繁多，需要对其进行仔细的记载。应该把记录接入

网络相关设备的日志信息，信息的内容一定要详细，对时间、事件、设备IP等要素都要进行详细的记载，并定期对日志信息进行核查，一旦发现问题，立即通知相关管理人员进行核查，将隐患扼杀在摇篮之中。并且要根据信息的重要程度进行分类，方便有效的进行查看，对日志信息的保留至少要达到三个月以上。日志需要对接入网络相关设备的登录和更改，并对其进行记录。

4.4设置口令进行加密

4.4.1对金融产业的重要资料和数据进行加密，设置口令，只有通过口令才能进行查看，只有相关工作的高层知道口令，一旦出现问题，就能立即缩小范围，找出出现问题的关键，不但能够保证资料数据的秘密性，还能将责任落实到个人身上，避免出现内部人员泄露的情况。

4.4.2通过口令对语句的控制来实现口令强度的增加，时间的持续性，密码条数的最大限制和登录失败的处置等，为了保证安全性，应当定期对口令进行更换，保证口令的安全性和适用应。

4.5设立独特身份

不同的系统设立一定的身份，只有登录独特的身份才能对数据进行修改拷贝，其他身份只有查看的功能，而独特身份不向公众展示，只有特定时期才会进行登录查看，这种方法有效防止内部人员和熟悉的黑客组织对金融机构下手。现管理

4.6设备登录

4.6.1远程登录进行限制。一般对金融业安全系统的攻击都是远距离或者海外，对远程的登录进行限制就能杜绝大部分的威胁。

4.6.2要限制远程登录的源地址。对于远程登录的登录地点进行限制，具体的做饭就是设立一定的登录地址，杜绝此外的地址进行登录。

4.6.3要设置登陆时间。对于登录时间有一定的限制，当规定时间过期之后，可以重新输出密码来进行登录，只允许合法的主机对数据一直可以进行运行，保证在其他IP登录时，能够进行有效的监管。

4.7路由认证

对于使用的路由器进行一定的限制，只有使用固定OSPF的路由器能够开启设备，并且开启过程中还需要认知，可以有效防止路由器被窃听或者是非法路的注入。

4.8故障定位与追溯

通过部署感知平台，对关键的设备进行监管，利用设备储存数据，在通过平台对数据进行分析，这样就能清楚的了解到问题出现的原因。姿态感知平台酒后对企业进行全面监控、分析、预警。态势感知平台能够将金融业的各种业务集中化进行监管，与每个应用的前端设备采集链路关联，并对其进行配置，保证每个应用的数据都能及时反馈。不但能达到整体、区域、单点全面监控预警的效果，还能提高工作效率。

5 结束语

网络的应用为金融业提供了很大的便利，但随之带来的威胁也是非常恐怖的。需要金融企业重视起安全管理的重要性，培养所有员工都具备隐私安全意识，努力避免网络威胁的发生，帮助金融业进入绿色发展，从而保障金融业的经济发展和公众财产不受到破坏。

参考文献：

[1]成维锋.新兴技术背景下金融业网络安全和监管面临的挑战[J].金融科技时代,2021,29(05):51-54.

[2]康一鑫,张林山,白雪莹.基于金融科技风险管控视角下的网络安全攻防演练研究[J].金融电子化,2020,(12):63-64.

[3]李彤.加强金融业网络安全风险管理的思考[J].金融电子化,2020,(11):18+20.

[4]王茜.网络金融下的金融管理模式探寻[J].全国流通经济,2020,(27):147-149.

[5]田家玺.完善网络安全管理机制推动我国金融业发展[J].商业文化,2020,(12):60-61.