档案网络服务安全技术架构应用研究

◎向 禹 吴世明

随着Internet技术和档案信息化的发展，越来越多的档案机构建立起网站、档案管理系统以及数字档案馆，通过互联网平台来展示自身的资源，通过网络来提升远程服务能力。档案馆的网络服务也越来越多地受到人们的关注。网络服务给用户提供方便快捷服务的同时，也面临着诸多安全问题的威胁。在做好档案资源开发利用、档案信息化建设的同时，必须加强档案网络服务的安全技术研究。

一、档案网站安全隐患分析

信息技术的发展，也带来了黑客技术和病毒技术的成长。由于操作系统和计算机程序存在的漏洞，也使得一些网站容易受到攻击。基于IIS网站的安全隐患大概有以下几个方面：

（1）Windows安全漏洞。Windows作为使用最广泛的操作系统，漏洞和针对它的攻击也是最多的。微软公司不断推出新的漏洞补丁，用户要及时更新最新的补丁。

（2）IIS安全漏洞。IIS是微软公司开发的基于Windows的WEB服务器软件，目前使用非常广泛，档案行业大部分网站都用它来组建网站，它同样也存在着很多安全漏洞，如Null.htw漏洞，微软数据访问组件（MDAC）执行本地命令漏洞等等都是高危的安全漏洞。

（3）黑客入侵。黑客对网站的入侵主要有两种类型。一是利用系统漏洞，通过端口扫描入侵系统，窃取敏感数据或者对系统进行破坏。二是利用现行网络的缺陷对网站进行诸如分布式拒绝

四、对《规定》贯彻落实的几点建议

1. 加大宣传贯彻力度。档案部门应加大宣传力度，针对特定人群开展专题培训，进一步扩大《规定》的社会影响。同时也可将有关典型案例作为宣传题材，以案说案、以案学法、以案普法，真正使《规定》入脑入心，做到真知、真学、真懂、真用。加强对贯彻执行《规定》情况的执法检查和执法监督，对档案管理违法违纪行为依法依规进行严肃查处，对典型案件进行曝光，以达到查处一案、教育一片的作用，充分发挥《规定》的威慑力。建立执法执纪协调配合移交制度，明确监察机关、人事部门和档案业务部门在查处档案管理违法违纪案件上的职责分工，细化案件移送的具体工作程序，形成查办档案管理违法违纪行为的强大合力。

2. 健全落实长效机制。建立贯彻落实《规定》的组织领导和工作保障机制。明确由各级监察部门、人事部门、档案部门分管领导承担的领导责任，加强对贯彻实施工作的组织领导和与有关部门的协同联系，及时研究解决贯彻落实中出现的问题，探索建立档案部门与监察机关、人事部门联合办案制度和联席会议制度等行之有效的工作机制。建立《档案违法违纪案件报告制度》、《档案违法违纪案件备案制度》和《重大违法违纪案件通报制度》等配套制度。

3. 及时制定实施细则。结合并根据当前全省档案管理中存在的实际问题和需要，由省档案局负责，三部门联合，组织档案管理、监察执法、公务员管理、政府法制部门有关专家和一线档案工作人员对全省档案管理现状进行广泛调研，围绕《规定》列举的档案管理违法违纪情形，剖析本省的具体情况，出台《湖南省档案管理违法违纪行为处分实施细则》，进一步细化在档案的收集、保管、开放、利用等各个环节中可能出现的各种违法违纪情形的行政处分，使责任追究更具可操作性。同时，结合《规定》中的具体条款，及时修订《湖南省档案行政处罚裁量权基准》。

（作者单位：湖南省档案局）

服务（DDoS）攻击，短时间内使得网络流量急速提高，网络链路不堪重负从而导致网站崩溃。

（4）计算机病毒。计算机病毒是一种人为编制的具有特殊功能的程序，它能够破坏计算机正常运行的程序，它的特性主要有：传染性、隐蔽性、潜伏性和破坏性等。任何病毒只要侵入系统，都会对系统及应用程序产生不同程度的影响，从病毒的检测方面来看，它还有不可预见性。不同种类的病毒，它们的代码千差万别。尽管反病毒工具在不断更新和提高，但是病毒对于反病毒工具来说永远是超前的。

（5）网站设计的安全隐患。考虑网页编程语言的漏洞，在程序设计时采用安全的程序设计外，档案网站因其特殊性，在尽可能多提供档案信息服务时，需要考虑到一些特殊的网站安全设计。例如，考虑档案的密级和保管期限，进行严格的权限控制，根据用户的不同角色给予相应的目录及原文浏览权限。另外，有许多非涉密档案，也不宜在网络上公开。通过网络提供开放性档案的电子原文浏览会成为趋势，但必须设计相应的安全关口，确保数据安全。

（6）安全意识问题。网站安全不仅仅是个技术问题，更多的时候是意识和制度的问题。档案网站不仅要加强安全技术，更应该提高安全管理和安全意识，据调查，档案行业缺乏专业网站的安全管理制度和忧患意识，缺乏安全意识和缺乏专人管理，也是档案馆网站的安全隐患之一。

二、档案网络服务安全设计

1. 整体安全架构。采用不同的设备和不同的技术架构组建的网络服务，安全效果是不一样的，很多网络服务直接连接互联网，黑客很容易利用扫描程序发现网站主机的信息、开放的端口、存在的漏洞而进入网站服务器。采用路由虚拟服务器技术组建网络服务，将多种网络服务隐藏，通过路由虚拟服务技术转发，实现网络安全服务。

2. 安全设计实现。假设某网站开放的服务有WEB服务、邮件服务、FTP服务，WEB服务从数据库服务器和应用服务器上获取数据提供给WEB用户查询。

（1）网络地址分配。路由器的IP地址为202.187.64.161（公众网IP）。WEB服务器为192.168.1.101（内网私有IP）；应用服务器为192.168.1.102；数据库服务器地址为192.168.1.103；邮件服务器地址为192.168.2.104；FTP服务器地址为192.168.2.105。

（2）划分虚拟局域网（VLAN）。划分VLAN，有这么几点好处：①端口的分隔，即便在同一个路由器上，处于不同VLAN的端口也是不能通信的。这样一个物理的交换机或者路由器可以当作多个逻辑的交换机或者路由器使用。②网络的安全，不同VLAN不能直接通信，杜绝了广播信息的不安全性；③灵活的管理，更改用户所属的网络不必换端口和连线，只更改软件配置就可以了。有效控制了网络广播信息的传播，让广播只在一个小的范围传递，减轻了网络负担，同一虚拟网的用户可更高效通信；不同VLAN之间可以在路由模块配置访问控制策略，避免非法访问，提高网络安全性；与网络管理系统（NMS）结合使用，网络管理员可更有效管理网络，包括监视网络流量，控制网络分流和设置安全级别等。

服务器较多的情况下，划分VLAN安全性相对较高。假设4个二层LAN口划分成两个VLAN：1口到2口属于VLAN 1，3口到4口属于VLAN 2；VLAN 1的网关是192.168.1.1，VLAN 2的网关是192.168.2.1。分配方式如下：

```
#interface Ethernet1/0.1
ip address 192.168.1.1 255.255.255.0
vlan-type dot1q vid 1
#interface Ethernet1/0.2
ip address 192.168.2.1 255.255.255.0
vlan-type dot1q vid 2
#interface Ethernet1/1
port access vlan 1
#interface Ethernet1/2
port access vlan 1
#interface Ethernet1/3
port access vlan 2
#interface Ethernet1/4
port access vlan 2
```

（3）配置公网地址转换。将服务器所处的内

部私有网络地址转换成可与外部 Internet 连接的公网地址。

```
#acl number 2000
rule 0 permit source 192.168.1.0 0.0.0.255
rule 1 deny
#interface Ethernet1/0.1
ip address 192.168.1.1 255.255.255.0
#interface Ethernet1/0.2
ip address 192.168.2.1 255.255.255.0
#interface Ethernet3/0
ip address 202.195.165.161  255.255.255.0
nat outbound 2000
```

（4）虚拟服务器配置。将内部私有网络的每种服务器的服务通过端口映射到路由器上，使外部网络访问某种服务时，将按照以下规则转发数据包，没有映射服务的数据包将被路由器丢弃。

［Ethernet3/0］ nat server protocol tcp global 202.195.165.161 www inside 192.168.1.101 www

［Ethernet3/0］ nat server protocol tcp global 202.195.165.161 ftp inside 192.168.2.105 ftp

［Ethernet3/0］ nat server protocol tcp global 202.195.165.161 25 inside 192.168.2.104 25

［Ethernet3/0］ nat server protocol tcp global 202.195.165.161 110 inside 192.168.2.104 110

……

（5）默认端口修改。采用虚拟服务技术，很容易管理IP的各个端口。通常将易受攻击的默认端口修改成陌生的端口，保障网络安全。如将内网的WEB服务映射成8800端口；FTP服务映射成2828端口；数据库服务映射成1485端口等等。

3. 优势分析。不管是计算机病毒，黑客入侵，还是系统本身存在的漏洞，攻击者往往先通过程序扫描搜集主机的有关信息，检查开放了哪些端口，有哪些端口可能进行攻击。通常通过端口扫描很容易发现服务器开放的端口。

通过这种架构可以看出，所有的服务器都处于内网，而暴露在外的只有路由器或防火墙，因此攻击者看到的信息也只是路由器的主机信息。对外开放的端口，只有80、21、25、110这四个端口，而数据库服务器是通过WEB服务调用，不直接与外界连接，外界根本无法获取数据库端口信息；即使是必须暴露某些端口，也可以将默认端口修改成攻击者无法识别的端口。所有的服务器处于路由器保护之下，在外界看来，只有一台服务器在运行，它就是我们用作虚拟服务器的路由器。外界不能直接攻击处于内网的服务器。相对于直接连接在Internet上的服务器，采用虚拟服务技术的网站架构要安全得多。

三、网络服务安全管理

网站安全还可采用防火墙技术、入侵检测技术等。也可以采用不定时人工干预，作为网站管理员，还需要不定时地对网站服务器进行查看，查出哪些文件夹容易被黑客写入程序或者修改，然后将此文件夹的权限设置为只读模式，也可以起到阻止黑客修改网站的作用。

要解决档案网站安全问题，除了使用安全产品，使用安全技术外，还必须加强档案网站安全管理：①增强安全意识；②加强网站及整个局域网的安全管理；③网站管理员要不断学习新技术，特别是防御攻击的新技术，做到防治结合。从安全隐患分析、安全技术、安全设计等多方面来综合考虑，单一的网络安全技术和网络安全产品无法解决网站安全的全部问题，需要将多种技术综合运用。档案网站安全是一项系统工程，有空间跨度，还有时间跨度，进行了安全配置与管理的网络系统并不是绝对安全的。随着时间推移和技术的持续发展，其安全状况也在发生相应的变化，只有让安全意识、安全技术和安全管理贯穿整个过程才能做到最大程度上的安全。

参考文献：

［1］Andrew S.Tanenbaum. 计算机网络（第4版）. 清华大学出版社2004.

［2］何小波. 网站安全问题及其防护措施分析. 现代商贸工业2009（2）.

［3］翟光. 公司网站安全防护系统解决方案. 信息与电脑（理论版）2009（9）.

［4］华为路由器和防火墙配置命令总结. 太平洋电脑网http：//www.pconline.com.cn/

［5］向禹. 基于SOA的高校档案资源管理系统研究与实现. 电子技术与软件工程2013（12）.

（作者单位：中南大学档案馆）