企业 Web 网站的安全策略

尹卫东 (河南省教育信息中心)
付保川 (河南大学计算机应用研究所)

摘要:本文针对 Web 网站所面临的安全问题,详细讨论了企业 Web 网站的安全策略,并给出构造企业 Web 网站的具体方案。

关键词:Web 网站 安全策略 防火墙 管理

一、引 言

随着 Internet 的日益普及和政府上网工程的快速推进,越来越多的政府机关、企事业单位都先后建立了自己的信息网站,并将本单位的有关信息通过 Web 网站发布出去,成为 Internet 的共享信息资源。但是,如何保证 Web 网站信息的有效性和安全性,是目前 Web 网站建设中人们普遍关注的问题。本文以政府部门和企事业单位 Web 网站(以下简称企业 Web 网站)的建设为例,谈一谈 Web 网站的安全策略。

二、Web 网站所面临的安全问题

信息资源的共享与信息安全历来是一对矛盾,向 Internet 网上提供的共享信息资源越多,对网站构成的安全威胁也就越大。影响 Web 网站安全的因素很多,有企业网络外部的、企业网络内部的、Web 网站自身的、网络管理方面的、网站维护方面的等等,大致可以归纳为以下几类:

(1) 企业网络外部的威胁:闲游用户的好奇闯入;信息间谍的恶意闯入;怀有恶意用户的闯入。

(2) 企业网络内部的威胁:内部用户有意的安全威胁;内部用户无意的安全威胁。

(3) 网站自身的问题:网络结构不合理;系统设置不正确;所采用的协议本身安全性不高;没有采用先进的网络安全技术、工具、手段和产品。

(4) 网络管理方面的问题:网络管理员对高级别用户的上网口令管理不严格,留给非法用户以可乘之机;上网信息的审查制度不完善或由于编审人员的疏忽大意,造成对信息的审查、管理不严格,从而导致秘密信息的泄漏;网站的信息维护不规范而导致对信息资源的破坏等。

面对上述问题,近年来各大公司先后推出了大量的网络安全产品,如 HP 公司推出了 NORMAN 防火墙产品;Digital 公司推出 TUNNEL 技术和 Digital's Firewall Service 防火墙产品;Checkpoint 公司推出 Checkpoint Firewall -1 高效、高性能的防火墙产品;Cisco 公司推出 Centri 和 PIX Firewall 系列防火墙产品;Microsoft 公司推出 Proxy Server 代理服务器软件产品等。

使用这些产品可以为增加网站的安全性提供技术保障,因此,在考虑 Web 网站的系统解决方案时要有针对性地选择一些网络安全产品,来提高 Web 网站的安全性。

三、企业 Web 网站的安全策略

Web 网站建设是一项综合性的工程,既包括网站的硬件、软件环境建设,又包括网站信息的组织、发布、管理和维护。因此,企业 Web 网站的安全策略也是一个综合性策略,它不仅要求在技术上采取必要的安全防范措施(例如构建防火墙等),更强调加强网络管理、信息管理和人员管理,健全安全管理机制,消除人为的安全隐患。

1. 整体设计完备策略

对 Web 网站的安全性设计从一开始就要纳入系统的总体规划和设计之中,而不是在系统建成之后再修修补补。安全总体设计应从网络结构的完整性,软件系统平台和开发工具的可靠性,网络管理和信息管理的规范化、制度化,以及信息维护(需要制作专门的信息维护工具)的方便性和规范性等方面来综合考虑。

2. 充分利用系统平台的安全防护机制

要提高 Web 网站的安全性,应首先考虑充分利用软件系统平台所提供的安全防护功能,实现不同层次的安全防护。例如 Windows NT 和 IIS 的配合就能提供较好的安全防护机制。

3. 构建合适的防火墙

根据各单位已有的计算机基础和对信息安全的不同要求，可以考虑设置多道防火墙，建立不同级别的信息安全区。一般情况下，政府部门和企事业单位均有自己的办公局域网（或者准备建设），并要求将局域网和 Web 网站连通。因此，设置两道防火墙即可满足网络安全的需要，外层防火墙把 Web 网站和 Internet 隔离开，内层防火墙把企业 LAN 与 Web 网站进行隔离，且两道防火墙要选用不同类型的防火墙产品，以确保内部段具有较高的安全性。外层防火墙最好采用代理服务器的双重宿主主机方式，这有利于提高对 Web 网站访问的安全性。

4. 信息存储和服务功能的分布要合理

企业 Web 网站的信息可分为静态信息和动态信息两大类。将静态信息以静态页面的形式按部门存放于指定的子目录下（一个部门一个子目录），并且不能使用系统安装时的默认路径，例如安装 IIS 时生成的 Web 服务的主目录名为 \ InetPub \ wwwroot，应将此路径更名，以减少利用缺省路径攻击 Web 站点的可能性；动态信息存放于数据库中，可以通过 ASP 程序将其发布到 Web 页面，数据库应存放于相对安全的地方。

所谓服务功能的合理分布，是指 Web 服务器、Ftp 服务器、email 服务器和数据库服务器的安装位置要合理。安装位置的选择与服务器的性能、信息流量、系统投资等因素有关，应具体情况具体分析，例如在不增加硬件投资和信息流量不大的情况下，可以考虑将 Web 服务和 email 服务合并到同一台服务器上。但是，Web 服务器、Ftp 服务器和数据库服务器则应尽量分离，将这些服务安装到不同的机器上，以避免因某个服务器被破坏而导致所有的服务瘫痪。同时，应考虑将上述服务器纳入到不同的域中进行管理，以避免一旦非法用户获得了某一个域的管理员权限，就可以破坏整个系统。

5. 技术与管理并重策略

如前所述，Web 网站的安全涉及多种因素，仅仅从技术方面考虑是远远不够的，必须采取技术与管理并重策略，加强网络自身的管理、上网信息管理和人员管理，建立安全管理制度，形成完善的安全机制。

在网络管理方面要设立专职的网络管理员。网络管理员要有高度的责任心，时常监视网络的运行状态，及时排查各种安全隐患。网络管理员要加强网络操作权限管理和用户口令管理，定期更改系统管理员或网络管理人员的口令。同时，对上网人员要加强安全意识教育，避免从内部网络对 Web 网站构成安全威胁。

6. 信息管理和维护的规范化策略

由于各个部门的职能不同，所提供的上网信息千差万别，因此实施规范化策略是保证上网信息有效性和安全性的必要手段。

首先，要制定统一的上网信息规范（如信息的分类办法、数据交换标准等），各部门共同遵守执行。

其次，信息的组织要有明确的分工，责任到人。对单位的信息组织要采取自上而下的方式进行，各职能部门在单位主页上是一个或几个相关栏目，各栏目的信息采集、整理、发布要由该部门的专人负责。

第三，成立信息编审机构，建立信息审查制度，严把信息入口关。

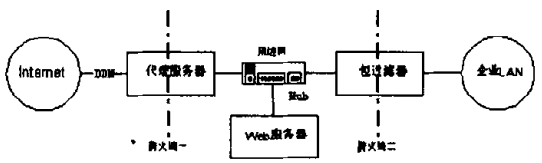
第四，信息的维护操作要规范化。各部门的信息维护要由专人负责并使用专门的维护工具。

四、构建一种安全的企业 Web 网站

Web 网站的安全性是政府部门和企事业单位的网站建设要解决的首要问题。针对 Web 网站所面临的安全威胁，在系统规划和设计之初就要把网站安全作为重要因素来考虑，并进行安全总体设计。我们在此推荐一种构建企业 Web 网站的系统解决方案，并具体说明对 Web 网站进行安全总体设计的思路。

1. 网络结构

作为信息发布和对外提供信息服务的 Web 网站实际上是一个由一台或几台 Web 服务器、电子邮件服务器构成的局域网。该局域网对外以 DDN 专线或其他连接方式与 Internet 相连，对内则通过应用网关或路由器与企业 LAN 连通。我们称这样的局域网为周边子网或 Web 网段，称企业 LAN 为内部子网或内网段，称 Internet 为外网或外网段。内网段对安全性的要求最高，Web 网段对安全性也有一定的要求，因此可以考虑在 Web 网段与外网之间、Web 网段与内网段之间，各构筑一道防火墙，且这两道防火墙的类型不同，如下图所示。



代理服务器采用具有双网卡的双重宿主主机（堡垒主机）方式，将 Web 网段与外网从物理上隔离，两者之间

的通讯必须经过堡垒主机来进行，而不能直接通信。这样，在外网上只能看到堡垒主机，而看不到 Web 网段，从而达到了保护 Web 网段和内网段的目的；数据包过滤器是防护内网段的第二道防火墙，可选用诸如 Cisco2514 这样的包过滤路由器。

这种双防火墙结构对内部子网具有相当高的安全性。即使堡垒主机被攻破，也仅只是给入侵者访问周边子网的机会，内部子网仍是相对安全的，因为入侵者连续突破两种不同形式的防火墙（尤其是不同厂家的产品）是相当困难的。

2.软件系统平台

软件平台的安全性主要由软件平台自身的安全机制来保障，因此应选用安全防护机制较完善的软件平台。根据政府部门和企事业单位的应用特点，我们建议采用如下方案：软件支撑平台选用 Windows NT Server 4.0，以 Internet Information Server(IIS)4.0 来构造 Web 服务器，以 Exchange Server 5.5 来构造电子邮件服务器，数据库采用 SQL Server7.0。静态页面制作工具使用 FrontPage98，动态网页开发工具选用 Visual InterDev6.0。

代理服务器的软件环境是 Windows NT Server 4.0、IIS 4.0 和 Proxy Server 2.0。

3.系统平台的安全防护功能

将服务器安装成主域模型，由主域（也称账号域）服务器负责对域用户的管理，Web 服务器、数据库服务器和电子邮件服务器分别建立各自不同的资源域，且不在资源域中单独设立帐户，以减少对这些服务器攻击的可能性。账号域和资源域之间建立信任委托关系，资源域为委托域，账号域为受托域，资源域对用户授予资源访问权限，换句话说，只有帐号域中的授权用户才有权访问资源域。为进一步提高系统的安全性，可以将主域服务器和数据库服务器放置于内网段中。

Windows NT 提供的安全防护机制是：

① Windows NT 用户账号和密码的安全保障。Windows NT 是通过分配用户账号和密码来保护系统资源和网络资源，也保护 IIS 不受侵犯，限制无关用户对 Web 服务器资源的访问权力，来保证 Web 服务器的安全；

② Windows NT 文件系统（NTFS）控制对文件夹和文件的访问。使用 NTFS 可以配置 Web 服务器的文件夹和文件的访问权限，禁止无关用户向文件夹中或从文件夹中复制、修改、删除文件，来保护 Web 服务器文件的安全；

③审查和监视 NTFS 文件和文件夹的未授权访问。利用 NTFS 可以审核和监视 Web 服务器的文件和文件夹的未授权访问（非法入侵）。

IIS 提供的安全防护机制是：

①Web 服务器的虚拟目录访问权限的安全设置。通过 Web 服务器的虚拟目录访问权限设置的选择菜单，可以设置虚拟目录的访问权限为读取和执行的组合。

②Web 服务器的用户访问控制和监视。将用户的访问控制设置为禁止匿名访问，即必须对远程客户请求进行认证，IIS 提供了三种类型的请求认证：基本认证（用户名和口令的传输、验证用明文，不加密）、Windows NT 请求/响应（用户名和口令的验证用密文）、安全套接字层 SSL（加密通过 Web 链路的所有会话信息）。可根据实际需要选择请求认证方式，一般选用第二种或第三种认证方式。

③Web 服务器的特定 IP 地址访问许可。通过配置 IIS，可以允许或禁止某些特定的 IP 地址对本 Web 服务器的访问。

利用 Windows NT 和 IIS 提供的安全防护机制，经过合理的配置与组合，可以较大幅度地提高 Web 网站的安全性。

五、结束语

网站的安全性是一个相对概念。实质上，在 Internet 网上没有哪个网站是绝对安全的，关键在于我们对待 Web 网站安全问题的态度以及采取什么样的安全策略。由于它涉及到网站规划、网站设计、网站管理和网站维护的各个方面，因此对这个问题的解决必须站在全局的角度予以高度重视。

参考文献

[1] D. Brent Chapman & Elizabeth D. Zwicky 著，构筑因特网防火墙，电子工业出版社

[2] Chris Hare & Karanjit Siyan, Internet 防火墙与网络安全，机械工业出版社

[3] Lee Hadfield 等著，Windows NT Server 4 安全手册，机械工业出版社

[4] 杨乔林，Internet/Intranet 中的 Web 服务器安全机制，计算机系统应用，1999 年第二期

（来稿时间：1999 年 6 月）