

关键词：政府网站安全

内容概要：

网络安全正在成为影响国家安全，成为渗透、影响甚至决定其他领域发展和成败的重要因素之一。加强政府网站安全建设刻不容缓，要着力构建一个技术先进、管理高效、安全可靠的政府网站安全保障体系。我国政府网站面临的安全形势非常严峻，其面临的主要风险从原来...

正文：

网络安全正在成为影响国家安全，成为渗透、影响甚至决定其他领域发展和成败的重要因素之一。加强政府网站安全建设刻不容缓，要着力构建一个技术先进、管理高效、安全可靠的政府网站安全保障体系。

我国政府网站面临的安全形势非常严峻，其面临的主要风险从原来页面被篡改、线业务被攻击、数据被窃取、内网被侵入的基础上，近几年来网站被攻击主要呈现的新特点：

一是攻击者攻击手段日益隐蔽。网络罪犯将会选取一些知名、响应不够及时的网站，作为第一攻击目标，而后利用从第一攻击目标上获得的信息再去访问最终的攻击目标。

二是攻击者逐渐从网络层攻击转向应用层渗透和攻击，这对Web应用防护必将提出更为严峻的挑战。现阶段的网站安全解决方案无一例外的把重点放在网络安全层面，致使面临应用层攻击发生时，传统的网络防火墙、IDS/IPS等安全产品对此类攻击的防御几乎不起作用。

三是攻击者的动机从个人爱好或是扬名到追求经济获利的重大转变。黑色产业链的形成与逐渐壮大已经成为网络安全必须面对的问题，部分不法分子为实现非法目的，不惜高价雇佣黑客修改、添加、删除私人信息，使得此类政府网站易于成为黑客攻击的对象。



政府网站存在的安全问题仍然不容乐观，产生这些问题的主要原因有以下三点。

1.网站管理机制不健全

管理机制主要包括制度、机构和人员三个方面，人员技术水平是否达到工作要求，是否把安全作为网站工作的重中之重来抓，制度是否落实到位，是否认真执行，都要靠健全的安全管理机制保障执行。

目前，政府各部门网站处于分散管理，仅有十几家政府网站托管在市政府网站平台统一管理，其余网站均自行维护，由于部分网站缺乏专业网络技术维护人员，网络技术水平不一，管理不到位，加之没有形成一套行之有效的监管机制，导致网站出现安全问题不能及时处理和解决。

2.网站人员技术水平有限

信息技术飞速发展，黑客攻击手段越来越高，网站工作人员技术水平与现时期工作要求还有一些差距，具体表现为：一是网络维护

人员在网络通讯设备和网络服务器配置上使用方法不当，导致网络硬件被黑客攻击；二是网站技术人员程序编写不够严密，导致应用系统被侵袭利用；三是网站技术人员安全防范技术能力不够，需要及时更新网络安全知识和业务技能；四是网站资金投入较少，网络硬件陈旧，软件应用新技术更新缓慢，不能适应当前网络安全新形势。

3.网站运维人员安全意识薄弱

目前，各部门政府网站还处于网站功能建设阶段，很多部门重建设、轻维护、重应用、轻管理的现象比较严重，对网站功能建设要求较多，主要精力投入功能实现上，从而忽略了代码质量，垃圾代码过多导致安全隐患问题。同时，网络维护人员、信息工作人员密码安全意识薄弱，防控病毒意识不强等原因也给网站安全带来极大风险。

构建网站安全防护体系，保障政府网站安全运行

针对上述政府网站面临的严峻形势和目前存在的主要安全问题，需要从涉及信息安全的人、管理、技术三个方面入手，要建立一个完善细致的安全防护体系,来保障政府网站平台安全稳定运行。

1.加强政府网站安全工作组织领导，提高责任意识

从每年开展的政府网站绩效考核工作可以看出，有相当数量部门领导没有把政府网站建设和安全管理工作作为一项重要工作来抓，存在重建设轻管理的问题。借鉴全国其他省（市）的先进经验，一是建议市政府将政府网站纳入地方政府和部门绩效考核体系，作为领导班子综合考核评价的内容之一，作为领导干部选拔任用的依据。二是要按照谁主管谁负责、谁运行谁负责的原则，强化管理和明确责任，确保政府网站安全管理工作落实到人，一层抓一层，做到网站管理不缺位，信息安全有保障。

2.建立健全政府网站安全管理制度，认真贯彻执行。

一是建立政府网站的安全管理制度体系，指导和制约网站安全建设和管理工作。网站出现相关问题时，工作人员要快速向网站相关负责人反映，以便及时得到处理；二是建立网站日常巡检制度，指定人员每日检查网站运行情况，及时发现并妥善解决存在的问题；三是建立具体负责人制度，对网站的网络管理、数据库服务维护、信息处理等实行谁主管谁负责；四是建立节假日值班制度，做到信息及时更新，保证网站不间断运行；建立日志记录备案制度，对网站日常工作要如实记录，并作为技术管理档案保存。

3.加强人才队伍的培养，统筹建立应急处理体系

一是加强政府网站安全管理培训。通过参加信息安全、信息技术、信息管理等方面的培训，进一步提高网站工作人员整体建设网站、管理网站的能力。二是强化技术支撑保障工作。成立信息安全测评中心，为党政机关、企事业单位网站提供技术保障和技术支撑服务。三是建立政府网站专项应急预案，以保证政府网站在事故发生时得到快速、及时处理。四是建立信息安全检查监督机制。依据已确立的技术法规、标准与制度,定期开展信息安全检查工作,对检查中发现的违规行为,按规定处罚相关责任人,对检查中发现的安全问题和隐患,明确责任部门和责任人,限期整改。

4.统筹规划政府网站群建设，实施集约化管理。

积极推进云模式下政府网站群的集约化建设。一是按照电子政务建设的总体要求，进行统筹规划，统一网站运行载体，避免分散、重复建设，即：利用信息中心平台的基础环境作为政府网站运行载体；由信息中心平台的技术队伍，承担政府网站的建设及日常运行的技术维护工作；对于缺乏建设、维护网站能力的单位或部门，不再建设独立网站，由信息中心平台代为承载其应向社会公众提供的政府信息公开等政务公共服务功能。二是确立统一标准，完善政府信息公开和政务信息资源共享机制，规划“中国”门户网站群及内容管理系统建设，进一步整合各部门政府网站，按照统一规划、分步实施的原则，建立统一的站群管理平台，将各政府机构网站整合到站群平台上运行，形成以市政府门户网站为核心，以政府机构网站为群体的，资源共享、协调联动的网站群体体系，全面提高政府网站公共服务水平。三是加强网站群建设管理，强化安全保障，建立应急响应机制，依托由信息中心平台现有技术、人才优势，为政府网站建设单位提供安全技术支持、信息技术培训、网络安全风险评估等服务。

5.加大安全技术体系建设

技术防护是确保网站信息安全的有力措施，在技术防护上，主要做好以下几方面工作。

一是要加强网络环境安全。首先要安装网站防火墙（WAF）、网站防篡改系统、网络防火墙和入侵检测系统等，在传统的网络防火墙基础上，网站防火墙（WAF）从网络的应用层面提高网站安全防护能力，利用入侵检测系统识别黑客非法入侵、恶意攻击以及异常数据流量,通过对网站防火墙（WAF）和网络防火墙进一步优化配置来阻断黑客非法入侵、恶意攻击。网站防篡改系统是网站最后一道防护屏障，一旦防护失效时，网站首页或内容被篡改，防篡改系统可立即恢复网站被篡改的内容，不至于造成政治事件和影响，同时给网站管理人员短暂喘息时间，及时修改和完善网站安全配置文件，确保网站安全稳定运行。

二是加强网站平台安全管理。在现有中心平台的基础上，进一步优化完善网络结构、合理配置网络资源，配置下一代防火墙、病毒防护体系、网络安全检测扫描设备和网络安全集中审计系统等设备，从边界防护、访问控制、入侵检测、行为审计、防毒防护、安全保护等方面不断完善信息化中心平台的安全体系建设，确保在信息中心平台基础环境下，大数据平台、大工业体系信息化辅助决策平台和云模式下政府网站群平台安全稳定建设运行。

三是加强网站代码安全。一个安全的网站，不但要有良好的网络环境，更要有高质量的应用系统，现时期由于网站代码不严密、安全性差引起的网络安全事件屡见不鲜，这就要求网站技术人员在开发应用系统过程中，要养成良好的代码编写习惯，尽量不要使用来历不明的代码和插件，编写程序时要严格过滤敏感的字符，并且在系统开发完成后，要有相应的代码检测机制和手段，及时更新漏洞补丁，从源头上遏制网站挂马、SQL注入和跨站点脚本攻击等行为。要部署网页防篡改系统，网页防篡改系统具备实时阻断非法修改和对非法修改的文件进行恢复的能力，在其他防护措施失效的情况下，能够有效地解决网页被篡改的问题，实现针对网站信息的保护。

四是加强数据安全。要加强数据库的安全，采用正版数据库系统，通过网络安全域划分,数据库被隐藏在安全区域,同时通过安全加固服务对数据库进行安全配置,并对数据库的访问权限做最为严格的设定,最大限度保证数据库安全；部署数据灾备系统，对网站和关键应用系统数据进行定期备份，利用市政府大楼机房环境，将这些数据进行异地备份，确保关键数据安全，防止造成无法挽回的损失。

随着信息技术的飞跃发展，黑客、木马等攻击和入侵手段也随之变化多样且层出不穷，给政府网站的安全管理带来极大的威胁，各级政府、各部门要切实增强政府网站安全责任意识，加强对政府网站安全工作的领导，进一步强化监督管理，明确责任分工，加强安全防范措施，以安全为己任，为政府网站和重要信息系统安全稳定运行创造一个良好的环境。

西安弈聪信息技术有限公司简介

西安弈聪立足陕西西安，为西安企业提供网站优化，软件开发，软件外包，电子政务，网站建设、企业网络营销咨询服务及实施为主体业务，为客户提供一体化IT技术服务。

西安弈聪现有技术架构包含PHP,asp,.NET.C++,VB,J2EE等，在MYSQL,MSSQL数据库系统，ORACLE大型数据库管理系统开发方面专长，经验丰富，是业内技术服务最全面，技术实力最雄厚的IT技术服务企业之一。

联系电话：029-89322522 4006-626-615 网址：<http://www.xaecong.com> 邮箱:admin@xaecong.com