学校计算机网络安全管理与研究

杜娟

（郑州工业技师学院　河南　郑州　450000）

[摘　要]随着我国现代信息化校园的不断建设，越来越多的学校开始实行信息化管理。信息化校园不仅给学校的老师以及办公人员带来极大的效率的提升，同时对于学生的生活也带来了便利，但是信息化校园的建设在也为学校的信息系统的安全性提出了更严格的要求。学校的网络安全管理不仅仅是保障信息系统的正常使用，使其不发生网络安全事件，应该更加注重网络安全管理的调整，使其在规避风险的同时构建良好的网络安全防护体系，从而整体化提升学校的网络安全管理能力，全面保障学校信息系统的网络安全。

[关键词]学校；计算机网络；安全；安全策略

【DOI】10.12252/j.issn.2096-6261.2021.06.287

一、网络安全的概念

何为网络安全，网络安全是指信息系统在到受外力的攻击时依然能够保障信息系统的正常可用，此处的正常可用不仅仅包含了信息系统的软件，还包括信息系统的硬件以及数据不被破坏或恶意的篡改。网络安全的核心是保障信息系统的完整性，真实性，保密性和可控性。

完整性主要是指网络的各种数据未经授权不能进行更改，也就是说网络的信息在存储过程和传输过程中不能被修改、破坏和丢失。

保密性是指网络信息不被泄漏给非授权用户。

可控性是指授权方对于网络的传播和内容具有可控制的能力。

可用性是指授权方能根据实际需要来改变网络的实际使用功能和范围。

二、学校常用的网络安全技术

（一）防火墙

防火墙主要是指局域网系统和外部互联网进行连接时设置的安全防线，在不同网络加设的系统整合等。防火墙的作用是保证让符合要求的信息通过，不符合要求的信息被禁止通过，最终目的是保证网络资源的正常访问。

（二）入侵检测系统（IDS）

该系统是对用户使用网络时进行的各种安全监测。在最近几年，由于各种网络入侵技术的全面提升，IDS的研究成了网络安全领域的研究重点。

IDS在计算机网络系统中被用来收集重要信息，从而找到网络和系统中不安全的隐患和容易受到攻击的行为。对监测系统进行重新组合的方式就被称之为入侵监测系统。

（三）防病毒技术

由于计算机病毒是网络安全重要的危害手段。因此对于计算机的病毒防护是保证网络安全的重要领域。在病毒防护中主要包括单机防护病毒和网关病毒防护。对于单机防护而言，主要是通过单机的程序设定，单机的数据进行扫描，并将病毒库和数据进行对比，一旦发现病毒就采取隔离或消灭措施，从而保证单机系统的稳定运行。对于网关防病毒而言，主要是通过网关来进行。

三、校园网络安全现状

（一）网络规模大、用户多

随着校园信息化的建设，学校的网络也在逐步完善，并且随着学校网络覆盖范围的不断增加，学校对于自身的网络层级的规划也在不断增加，再加上学校人员的数量，学校信息系统的复杂性这就造成了学校的信息的管理难度，同时因为涉及的人员不仅仅包括学生还有学校的教职工等，用户的组成也相对较为复杂，这些都是使得学校的网络安全管理变得更加复杂。

（二）网络安全意识缺乏

信息化校园的建设给高校带来便利的同时，对于学校的网络安全建设也提出了更高水平的要求。而当前高校的信息系统的管理者对于网络安全的管理意识淡薄，往往只注重网络安全设备的架设，缺乏对于用户上网行为的管理。这使得虽然在外部来说能够有效防范网络攻击，但是由于内部人员的网络使用习惯的差异，造成木马的下载，从而感染蠕虫病毒等。因此，网络安全的管理不仅仅只依靠安全设备的部署加固，更多的要是对于使用人员的安全意识的培养，形成良好的上网习惯，避免网络安全隐患，加强网络安全防控。

（三）网络管理人员技能不足

目前很多高校的网络信息化管理较为混乱，特别是管理人员方面，缺乏统一的管理人员，不能落实专人专责的管理制度。在技能方面，因为网络管理人员缺少专业的技能培训，在管理方面网络管理人员虽然能力保障网络的基本运维工作，但是在遇到突发性安全事件时，缺乏一定的应急能力，而且对于学校的网络安全架构的建设，网络安全的管理方面技能较为缺乏，这也为学校的网络安全带来巨大的风险。

四、校园网络安全问题分析

（一）计算机硬件配置不足

由于高校领导对于学校信息系统的网络安全重视程度不足，这就使得对于学校的硬件设备的经费不足，学校的机房的硬件配置往往处于较低的水平。很多硬件配置对于正常的使用尚且不足，对于抵抗网络攻击更是存在问题。同时由于缺乏经费的提供，对于安全设备的购买和部署同样存在问题，信息系统缺乏网络安全设备的防护会使得信息系统暴露在网络攻击中，对于信息系统带来极大的安全风险。

计算机的硬件配置如计算机的内存，cpu等对于信息系统的运行起着十分重要的作用，硬件配置的不足往往会导致因为用户的过量访问或软件的运行而造成系统的卡顿，这不仅会给使用者带来极大的问题，同时对于安全软件的部署也存

在弊端。防护软件的部署一般需要依据信息系统自身的硬件配置作为支撑，从而对信息系统起到安全防护的作用，而配置较低的计算机硬件往往会因为自身的内存不足等问题无法正常部署防护软件，这也使得信息系统的安全防护处于较低的水平，从而带来极大的安全风险。

（二）病毒木马的侵害

网络安全事件是时有发生的，特别是近年来网络安全事件更是频发。勒索病毒、蠕虫病毒、俄洛伊木马等网络攻击的肆虐，对于各大高校，政府，企业等带来极大的安全风险。特别是从2015年以来，网络攻击事件更是成指数级增长。网络病毒木马有着极强的破坏力，不仅严重影响了信息系统的正常使用，同时会破坏其中的数据，对于信息系统造成永久性的损害。有些计算机病毒的潜伏期也是非常长的，即使中毒的计算机在一段时间内运行正常，但是在某一时间段就会爆发病毒，从而对计算机网络造成十分严重的危害。高校作为勒索病毒的重灾区之一近年来安全事件频发，高校作为保障学生个人信息的防护单位有义务去提升高校信息系统的安全防护能力，保障学生们的个人信息安全。因此，学校应加强学校信息系统的安全防护，为学生的个人信息安全提供有力保障。

（三）黑客攻击无处不在

随着信息技术的不断发展，为了谋取利益，很多黑客组织都会向着政府、医疗、电力、教育等基础单位进行攻击，而作为信息系统较为复杂多样且防护能力较弱的高校则更是成为黑客攻击的主要目标。在2021年上半年更是有多个高校遭受网络攻击，例如某科技大学的4万学生的信息在暗网售卖，其中包括了学生的姓名，学号，家庭地址等详细信息，更有数据显示，高校信息系统平均每天都要承受几十万次的网络攻击，而一些安全性较差的校园网，内部漏洞和安全管理技术能力缺乏，也容易被这些黑客攻破，从而使得校园网面临极大的安全风险。

这种网络攻击不仅仅来自校外，还有一部分来自内部。一些学生，为了学习网络安全技术，在实践的过程中往往会拿校园网来“练手”，从而磨炼提升自己的网络技能，而这种行为也会对校园网络带来极大的安全风险。在这种不安全的环境中，个人财产和个人信息被外泄。此外，由于黑客的频繁攻击，也容易对校园网造成瘫痪。

五、校园网络安全管理防范对策

（一）加大校园网络的管理和宣传力度

由于网络的参与人群是学校的教职工和学生，所以要确保这些学生和教师的安全上网是每一位学校网管都需要面对的问题。因此不论学校网管还是使用者，都需要加强对网络安全的防范意识。增强网络安全的基本理念。对于网络中的安全隐患能有最基本的识别能力，尽量不去点击非法链接，对于提示存在风险的网站也尽可能的不去浏览，网络使用者要尽可能在网络设备中添加防护软件。不论实在电脑上、手机上都需要安装网络防护软件，这样就能阻挡大多数网络病毒和攻击。

同时，学校网管要充分恪守职责，对于网络的安全隐患做到极可能高的控制，同时还需要对网络管理者进行必要的知识更新和培训，从而能够识别最新的网络病毒手段和网络攻击技术，从而做出有效的预防和维护。

最后，学校和工信部、教育局等部门也要加大对于网络安全的宣传和教育，通过多种渠道，例如网站、短信、微博、微信等方式进行网络安全有关知识的宣传。并通过大量的事实案例来提醒广大网友需要注意的事项，从而增强广大网络的上网安全意识。

（二）对网络风险加强管理

作为学校网络的管理者，要定期对学校网络进行安全维护。例如及时跟进发布的有关风险，对学校网络涉及的安全问题及时安装系统补丁，对防火墙策略进行有效的设计和优化。同时也需要基于自纠自查的方式，不断检查校园网络安全的漏洞，并及时进行修补。对于各种网络安全设备要进行定期的检查升级，对服务器、路由器、网关这些网络设备尽可能的提升网络权限，增加各种访问权限，并且对TCP协议进行必要的限制，对每个访问的IP进行必要的限速，也要对路由器进行合理的配置，充分过滤一些不必要的协议，从而降低网络风险的概率。在人员管理方面要建立完善的人员管理制度，对于人员的操作进行限制，对于用户的上网行为进行严格的监督，对具有恶意操作的上网行为进行及时的阻断，从而避免安全事件的发生。同时学校应当建立应急预案，对于突发性安全事件做到及时快速的反应，及时有序的恢复有关系统，确保学校的信息系统安全。

（三）定期对数据进行备份

数据是信息系统的重要组成部分，也是最为重要的部分，数据安全问题是信息系统最需要重视的问题，数据的安全性关系到信息系统整体的安全问题。而随着近年来勒索病毒事件的频发，对于数据的安全性问题一定要得到重视，学校应该定期对数据进行备份，从而在信息系统遭受破坏时能够第一时间对数据进行恢复，从而保障信息系统的可用性。学校要有专人对数据进行定期的备份，可以一个月备份一次从而保障数据的有效性，同时对于备份的数据要做异地的存储，这样在发生安全事件时不会涉及备份的数据，从而保障数据的安全。

结语

随着高校信息化的不断完善，对于高校的网络安全问题也提出了更加严格的要求。高校的网络安全管理问题也是学校管理应该重视的问题，学校要树立良好的网络安全意识，及时对数据，硬件，软件等进行安全管理和防护，从而保障信息系统的安全，这也是每个高校应尽的义务。没有网络安全就没有国家安全，只有不断加强教职工，学生的网络安全意识，提升网络安全管理人员的技术能力，才能更好的保障学校信息系统的安全，网络安全管理能力的提升依然任重而道远。

参考文献

[1]谢振坛，申伟.校园网络安全管理现状与对策探究[J].教学与管理，2019（18）：52-54.

[2]张超.校园网络安全管理及体系结构的研究[D].华东师范大学，2009.