# 新形势下企事业单位网络信息安全问题探讨

郭海龙
广州市城市规划展览中心　广东省　广州市　510000

**摘　要：**信息时代的到来使网络安全问题成为社会各界关注的重点，如何保障网络信息安全成为我们需要探究的重点问题，解决这一问题对提升网络安全防护能力，净化网络环境具有重要的意义。尤其对于处在新形势下的企事业单位，其网络信息安全关乎生存，关乎工作开展，因此显得尤为重要。鉴于此，本文分析了保护企事业单位网络信息安全的必要性，并且探讨了大数据时代下企事业单位网络信息安全的相关影响因素，最后提出大数据时代企事业单位加强网络信息安全防护力度的方式，希望为以后研究提供参考。

**关键词：**新形势；企事业单位；网络信息安全

## 1 引言

随着信息化时代的到来，我国网络信息技术得到了快速发展，使得人们的日常生活发生了极大的改变，但技术的发展和应用必然也伴随着挑战。如今，网络信息安全不仅会对整个网络环境造成影响，还会影响个人用户的使用。因此，网络信息安全问题需要个人、社会组织及政府机构的协调配合，从个人意识、技术手段及法规政策方面入手，加强网络信息安全防护能力。在网络信息安全管理的过程中，主要从两个方面来保障网络信息安全，一方面是加强计算机自身的安全防护系统，可以帮助过滤使用过程中出现的不良信息和不利因素，另一方面可以通过外部防御设备防止外来系统对计算机自身系统进行更改。

目前，我们所处的网络环境并不是十分友善，在网络中仍然存在着信息买卖、资料泄露等情况，这些都会使网络环境进一步恶化。对此，需要相关部门和社会组织借助法律法规、技术手段改变现有的网络状况，比如加大对网络安全违法违规行为的整治力度，强化威慑能力；比如完善内部网络安全管理的规章制度，加强约束能力。只有逐步的推动网络信息安全相关工作的开展，才能营造良好的网络环境。

## 2 保护企事业单位网络信息安全的必要性

目前，传统的工作方式已经逐渐被现代互联网工作方式所代替，企事业单位依托网络得以高速发展，产生的海量数据和信息存储在单位内部，来自网络的威胁无形无色，但却足以摧毁或者是影响企事业单位工作的开展。

过去几年，网络安全事件频发。如澳门卫生局电脑系统遭恶意攻击，影响健康码、核酸检测工作的开展；如台积电生产工厂和营运总部中勒索病毒，生产线全数停摆；又如西北工业大学邮件系统遭受境外网络攻击。这些网络攻击、信息泄露事件提醒我们要“警钟长鸣”。在使用过程中，计算机网络本身所具有的开放性以及脆弱性，始终威胁着企事业单位的信息安全。因此，我们有必要及时了解网络信息安全相关问题，并不断探索和挖掘对应的解决策略。

## 3 大数据时代下企事业单位网络信息安全的相关影响因素

### 3.1 网络的开放性特点

在大数据不断发展的今天，开放性作为计算机网络中的最显著特征，其在发展过程中也具有脆弱性的特点。由于开放性的网络无法全面保护计算机的网络安全，也无法全面保护企事业单位的数据信息，因此终端设备、网络系统和网络基础设备的安全性每时每刻都在收到来自内部或外部环境的威胁。

### 3.2 存在网络攻击、病毒侵扰的可能性

计算机网络技术全面普及，信息得到快速传播，黑客就是信息网络化时代的产物。在网络运行的过程中，黑客利用网络技术进行有目的的攻击行为，这种行为就属于恶意破坏，同时，该行为的针对性比较强，并且在实际攻击的过程中会对企事业单位网络信息的完整性和安全性造成极大的影响。通常情况下，黑客的攻击行为主要分为主动攻击和被动攻击两部分，其中被动攻击主要是对网络信息进行获取和破解，进而对网络信息的安全运行形成破坏。这两种攻击行为都会对信息安全造成极大的影响，使得数据丢失或系统瘫痪。

由于计算机网络是一个开放性的网络系统，这种开放性的特征使得信息可以进行大量的传播，病毒其实也是数据信息的一种。网络系统对病毒的入侵缺乏有效的防控，特别是在大数据信息时代下，病毒的隐蔽性使它很难被发现，当病毒入侵成功之后再发现往往为时已晚。

3.3 信息安全管理体系不够健全

当前形势下，计算机网络在企事业单位的日常工作中具有非常重要的地位，已经成为员工开展工作的重要依托。大多数企事业单位的信息安全管理仍停留在技术管理、外部防御阶段，对如何规范内部员工操作行为等缺乏必要的约束，内部防护手段不足，所以，要建立完善的信息安全管理体系，从内及外，以制度规范促进企事业单位网络安全防护能力的提升，防止网络信息安全问题的出现。

**4 新形势下企事业单位加强网络信息安全防护力度的方式**

4.1 努力构建完善的制度体系

要做好信息安全工作，完善制度建设是第一步。企事业单位要以问题为导向，结合网络信息安全工作不断变化的要求，梳理单位内部信息安全现状、明确内部信息安全职责边界，逐步完善计算机信息安全、软件使用、设施设备管理等方面的信息安全制度，尽可能扩大信息安全管理的覆盖面，以制度落地，推动信息安全工作的开展，要让制度成为单位内部开展信息安全工作的有力抓手。

构建完善的制度体系，并不意味“只构建不更新”，作为企事业单位，还要保持一定的更新机制，根据最新信息安全要求定期更新相关制度。比如，近些年，等级保护2.0标准发布，2.0标准相较1.0的不仅对象范围扩大，安全要求也有所不同，标准更为严格，更为全面。面对新要求，企事业单位要主动按照新标准要求对制度进行更新，确保制度管理方面能满足新标准要求，这也是主动落实单位信息安全管理责任的体现。这么做，一是通过更新制度，确保单位信息安全防护能力逐步提升，二是为了在如今越来越多的安全检查中也能“淡定”迎检。

4.2 狠抓信息安全工作落实

近几年，信息安全工作难度大大提升，稍不留神，就容易发生信息安全事件，这就要求企事业单位要时刻保持警醒，切不可麻痹大意，放松警惕。企事业单位在信息安全工作上，要从源头做起，从基础抓起，按照信息安全工作的要求，通过逐项对比自查自纠的“笨办法”，一点一点推落实。通过使用技术手段排查安全隐患的“新方法”，一点一点推改进。通过逐项逐项落实，逐条逐条改进，切实提升企事业单位的网络信息安全防护能力。

对于整体技术能力不够强的企事业单位，还可以邀请外部专业的第三方信息安全公司为单位“保驾护航”，请专业的安全技术人员对单位内部的网络信息安全现状做一次全面的分析，通过开展安全风险评估工作，找出目前安全防护体系的短板、重点业务系统存在的安全隐患、以及后续安全防护提升和完善的措施，找出问题并改进，以此推动信息安全工作的落实。

4.3 应用新技术，掌握新态势，强化信息安全防护能力

新形势下，不法分子掌握的病毒、攻击手段层出不穷，为最大化的提升防护能力，企事业单位要打破“能防一次就能防永久”的观念，及时应用新的信息安全防护技术。基础的“双防”要落实，要充分应用好防火墙技术和病毒防范技术，合理部署网络防火墙，科学配置安全策略，抵御外部攻击。对于网络应用，还应部署应用防火墙，加强恶意代码等应用层面攻击的防范能力。如有条件，还应考虑配置上网行为管理、代码审计、入侵检测、“零信任”等信息安全设备，利用技术手段提升各个层面的信息安全防护能力。

企事业单位要及时掌握最新安全态势，关注最新发布的安全漏洞，根据最新发布的漏洞补丁对单位内部相关设备进行修复，避免因修复不及时导致漏洞被不法份子利用，造成损失。

4.4 注重终端安全防护工作

我们都知道信息安全工作十分重要，但在大部分的企事业单位，信息安全工作并非主要业务工作，很多时候在信息安全方面的投入也并不是十分大，部分单位可能连基础的安全防护设备都无法部署，这种情况下，难道就放开信息安全工作，听之任之、消极应对吗？不是的，做好终端安全防护工作也能极大地助力信息安全。

要做好终端安全防护工作，一是要做好终端设备的摸查、排查工作，摸清“家底”，建立台账，确保一个不漏；二是逐台设备进行检查，主要做好操作系统安全基线检查，如检查启动项、主机防火墙、账号安全、端口开通情况等，对不必要的服务和账号要及时禁用和删除。对于服务器设备，还要做好数据库层面、中间件层面的检查；三是做好终端设备网络流量的监控，对于异常流量要重点关注，上机检查要抓包并分析其对应的应用，进一步判断应用安全性；四是要定期抽检终端设备日志，使用专业的日志分析工具分析，对日志异常的，要果断断连，避免传播范围扩大。

在大数据时代，为了能够降低网络病毒出现的概率，就要认识到开展终端设备安全防护工作的重要性，在对木马入侵源头进行严格管控的同时，逐步加强身份验证、主机防护等功能。针对终端，除了安装防病毒软

件外，还应开启主机防火墙，合理配置防火墙进出站策略。此外，还要及时对系统进行补丁更新，定期开展系统漏洞扫描工作，及时修复漏洞。有能力的单位还应统一管理，做到自定义安全基线，比如统一关闭不适用的服务和端口、统一配置主机防御策略等。其中账号安全是重中之重，数据显示七成左右的成功攻击操作都是弱口令导致的。如今计算机性能高度提升，密码爆破能力大大加强，稍弱的、有规律的密码很容易被爆破成功，从而导致内部网络被入侵。因此，终端账号安全是最简单但往往也是最容易忽略的一步，检查账户密码，确保满足密码强度要求是最基本的信息安全要求。

4.5 重视培训教育，规范日常操作

要清醒地认识到堡垒最容易从内部攻破，信息安全不仅仅是一个人、一个部门的事情。提升信息安全理念，落实信息安全工作，单位内部全体职工都责无旁贷。企事业单位要开展常态化信息安全教育培训工作，可以以邀请外部专家、结合单位实际自行宣讲等方式组织网络信息安全培训，培训内容不固定，可以是信息安全案例分析，也可以是办公信息安全培训，还可以是信息安全技术培训，以培训的多样性提升培训的吸引力。日常要注意多做提醒工作，以“温馨提示”方式给单位员工打入“提神针”，提醒全体员工提高警惕，学习识别网络钓鱼、网络欺骗等常见攻击手段，未经识别的邮件内按钮、链接、附件，一律不轻易点击，点点提醒融入生活、工作，努力帮助员工克服松懈麻痹思想，规范全体员工的日常计算机操作行为，形成单位内部“防护圈”。单位还应定期组织信息安全演练，制定不同的演练脚本，召集员工参与到演练中来，除了内部人员，还应邀请外部支撑单位相关人员参与并建立联络机制，及时通报传达相关信息，提升内外协同处理能力的同时，提升单位整体信息安全应急处置能力。

4.6 加强网络监测与监控

要想第一时间发现网络信息安全事件，毫无疑问就必须借助安全防护设备开展网络监测与监控工作。开展网络监测与监控的主要作用是在日常运行的过程中监测内部系统是否被攻击，数据信息是否被盗用，是为了对发现的攻击行为进行确认，并能详细记录攻击相关数据。根据监测到的安全事件，企事业单位要提高重视，及时进行分析和确认，根据分析结果，考虑可能产生的其他攻击事件，并及时做好防护，确保被攻击对象的安全。同时，对于经过分析并确认的攻击事件，将其涉及的IP地址、攻击方式、攻击行为等威胁情报整理后应主动将情报进行共享，避免同行业或存在联系的其他单位被攻击，进而影响整体业务开展。在加强监测监控的同时，为更好的处理信息安全事件，企事业单位也应加强安全事件和重大故障的快速相应和处理能力，通过应急演练等形式去强化应急处置能力，避免只能监测监控无应急处置手段的局面发生。

常用的网络监测与监控为统计分析法与签名分析法。前者基于数理统计知识，分析对象是计算机网络系统中的动作操作模式，能够第一时间发现系统运行过程中存在的危险因素与异常行为；后者的分析对象是针对系统弱点进行攻击的现象。在企业与行政事业单位中，网络监测与监控技术十分常见，是一种十分高效的计算机网络信息安全保护技术。

## 5 结语

综上所述，网络信息安全防护工作是新形势下的必然要求，也是保护企事业单位各类数据信息、使企事业单位保持稳定运营的关键。企事业单位存在的问题不外乎网络安全防护体系不完善、网络安全管理意识不到位、管理责任落实力度不够大、网络安全防护监测能力不够强几个方面。为了加强单位的信息安全防护能力，要抓好制度建设完善，要抓好信息安全工作落实，要通过应用新技术，掌握新态势，抓好信息安全防护能力提高，要注重终端防护工作开展，抓好信息安全工作之基础，要通过培训教育、规范日常操作，抓好全员信息安全意识的提升，要通过日常网络监控，抓好信息安全监测分析能力的提升……新形势下，网络信息安全给企事业单位带来新的挑战，让我们共同努力，为企事业单位、为国家打造更为安全的网络环境。

**参考文献：**

[1]王伟然,李芝语.计算机网络信息安全问题探讨[J].软件,2021,42(07):108-110.

[2]熊涛.大数据时代下计算机网络信息安全问题探讨[J].电脑编程技巧与维护,2020(10):160-161+167.DOI:10.16184/j.cnki.comprg.2020.10.062.

[3]赵蓉英,余波.网络信息安全研究进展与问题探析[J].现代情报,2018,38(11):116-122.